Cyberster

INTERNSHIP REPORT

A Weekly Progress and Learning Summary

Phase Two : Browser Forensics, LNK File Analysis, and Artifact Integration

Submitted to: Cyberster Internship Program

Intern Name: Abdul Muqeet Tabraiz

Roll Number: CSI-B1-353

Browser History Analysis | LECmd (LNK) | JLECmd (Jumplist) | SBECmd (Shellbags) | Artefact Timeline Integration | Cross-Artefact Correlation

A Weekly Progress and Learning Summary

Table of Contents

Cyberster Blue Team Internship — Week 9

Week 9 Overview

Week 9 of the Cyberster Blue Team Internship transitions Phase Two of the program from system-level artefacts (Event Logs, Prefetch, MFT) into application-layer evidence. The week is structured into three investigative parts, each performed live on the analyst's endpoint to reproduce a realistic Digital Forensics and Incident Response (DFIR) workflow.

Part A (Days 60–62) covers Browser Forensics, where Chrome, Edge and Firefox profile databases are collected, hashed for evidence integrity, and then parsed with DB Browser for SQLite, BrowsingHistoryView, ChromeCacheView and MZCacheView to reconstruct user web activity, downloads, cookies and cache entries.

Part B (Days 63–65) covers LNK File and Jump List Analysis, using Eric Zimmerman's LECmd and JLECmd to parse Shell Link metadata for evidence of removable media, network share access, and file usage history. Volume serial numbers and target file paths are correlated to identify USB devices and unusual file access patterns.

Part C (Day 66) integrates every artefact from Weeks 7, 8 and 9 into a single unified investigation timeline. After timezone normalisation (Local → UTC), entries are cross-correlated across artefact sources to demonstrate how a forensic narrative is reconstructed end-to-end.

Critical Warning Followed All Week: Before working on any browser, ALL browser windows were closed and every chrome.exe, msedge.exe, firefox.exe and brave.exe process was terminated in Task Manager. Browsers run background processes that keep SQLite databases locked even after windows close — failing to terminate them would have produced empty parse results.

Timezone Discipline: Nirsoft tools (BrowsingHistoryView, ChromeCacheView) export in Local Time (PKT, UTC+5). EZ Tools (LECmd, JLECmd) export in UTC. All Day 66 timeline entries were converted to UTC before merging to prevent corrupted correlations.

Part A — Browser Forensics (Days 60–62)

Objective

The objective of Part A was to perform a complete forensic acquisition and analysis of the browser artefacts present on the analyst's local Windows 10 endpoint. This included identifying installed browsers, locating profile databases, performing forensically sound copies with robocopy, generating SHA-256 evidence hashes, parsing SQLite databases (History, Cookies, Web Data) and exporting unified history, cookie, cache and extension inventories.

Tools Used

- Windows 10 Host Machine — Target endpoint for live forensic acquisition
- Command Prompt (Administrator) — Folder creation and acquisition
- PowerShell (Administrator) — SHA-256 hashing with Get-FileHash
- robocopy — Forensically preserved copy with /COPYALL /B switches
- DB Browser for SQLite (sqlitebrowser.org) — SQLite database inspection and CSV export
- BrowsingHistoryView (NirSoft) — Cross-browser history aggregation
- ChromeCacheView (NirSoft) — Chrome and Edge cache parsing
- MZCacheView (NirSoft) — Firefox cache parsing
- Microsoft Excel — Filtering, sorting and timeline construction

Phase 0 — Tooling and Environment Preparation

Step 1: Download Required Forensic Toolkit

All required tools were downloaded prior to Day 60 and extracted to C:\Forensics\Tools\. No installation was required for the NirSoft and EZ Tools utilities. The complete toolkit table is shown below.

Tool	Source	Used In
BrowsingHistoryView	nirsoft.net	Days 60–62
DB Browser for SQLite	sqlitebrowser.org	Days 60–62
ChromeCacheView	nirsoft.net	Days 60–62
MZCacheView	nirsoft.net	Days 60–62 (Firefox)
LECmd (EZ Tools)	ericzimmerman.github.io	Days 63–65
JLECmd (EZ Tools)	ericzimmerman.github.io	Days 63–65

Phase 1 — Browser Detection and Profile Collection

Step 1: Identify Installed Browsers

A non-elevated Command Prompt session was used to enumerate which browsers were installed on the endpoint. The dir command was run against each browser's expected installation path; the && echo conditional only fired when the executable was successfully located.

```
dir "C:\Program Files\Google\Chrome\Application\chrome.exe" 2>nul && echo Chrome FOUND
dir "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" 2>nul && echo Edge
FOUND
dir "%PROGRAMFILES%\Mozilla Firefox\firefox.exe" 2>nul && echo Firefox FOUND
```

```
dir "C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe" 2>nul && echo Brave FOUND
```

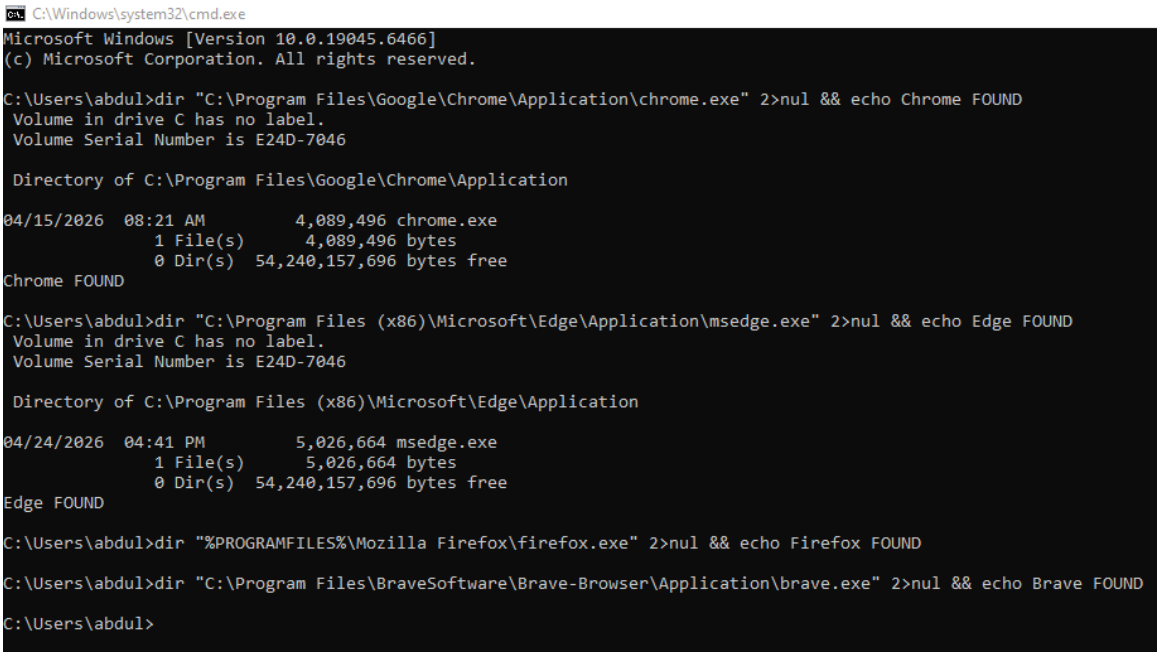


Fig 9.1 — Browser detection output. Chrome and Edge confirmed installed; Firefox and Brave returned no path (not present on endpoint).

Step 2: Locate the Exact Chrome Profile Path

Chrome was opened and the address chrome://version was used to read the live Profile Path field, which confirmed the active profile location at C:\Users\abdul\AppData\Local\Google\Chrome\User Data\Default. Personal username and identifying details were redacted before screenshot capture.

Fig 9.2 — chrome://version page showing Chrome 147.0.7727.102 (64-bit) and the verified Profile Path used as the acquisition source.

Step 3: Create Forensic Working Folders

An elevated Command Prompt was opened (UAC), and a clean directory tree was created under C:\Forensics\BrowserForensics to hold each browser's artefacts and the consolidated CSV exports.

```
mkdir C:\Forensics\BrowserForensics
mkdir C:\Forensics\BrowserForensics\Chrome
mkdir C:\Forensics\BrowserForensics\Edge
mkdir C:\Forensics\BrowserForensics\Firefox
mkdir C:\Forensics\BrowserForensics\Exports
```

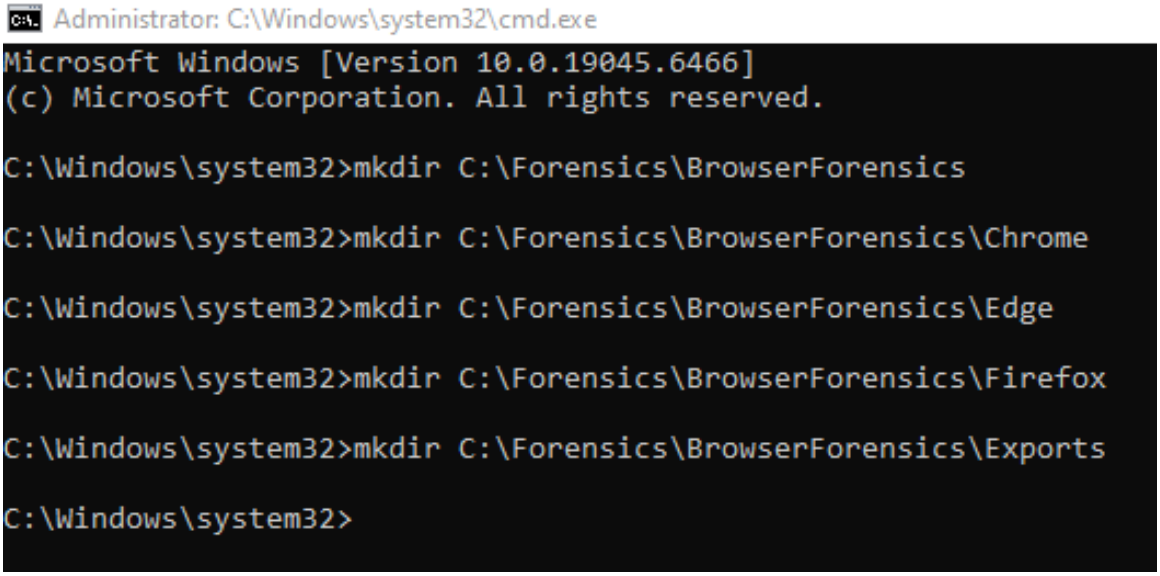


Fig 9.3 — Working folders created under C:\Forensics\BrowserForensics for each browser and a dedicated Exports directory for CSV deliverables.

Step 4: Close Browsers and Kill Background Processes

All browser windows were closed and Task Manager was opened (Ctrl+Shift+Esc) to confirm that no chrome.exe, msedge.exe, firefox.exe or brave.exe processes remained running. SQLite databases (History, Cookies, Web Data) are locked while the browser holds them open; failing to kill these background processes is the most common reason that downstream parsing tools return zero rows.

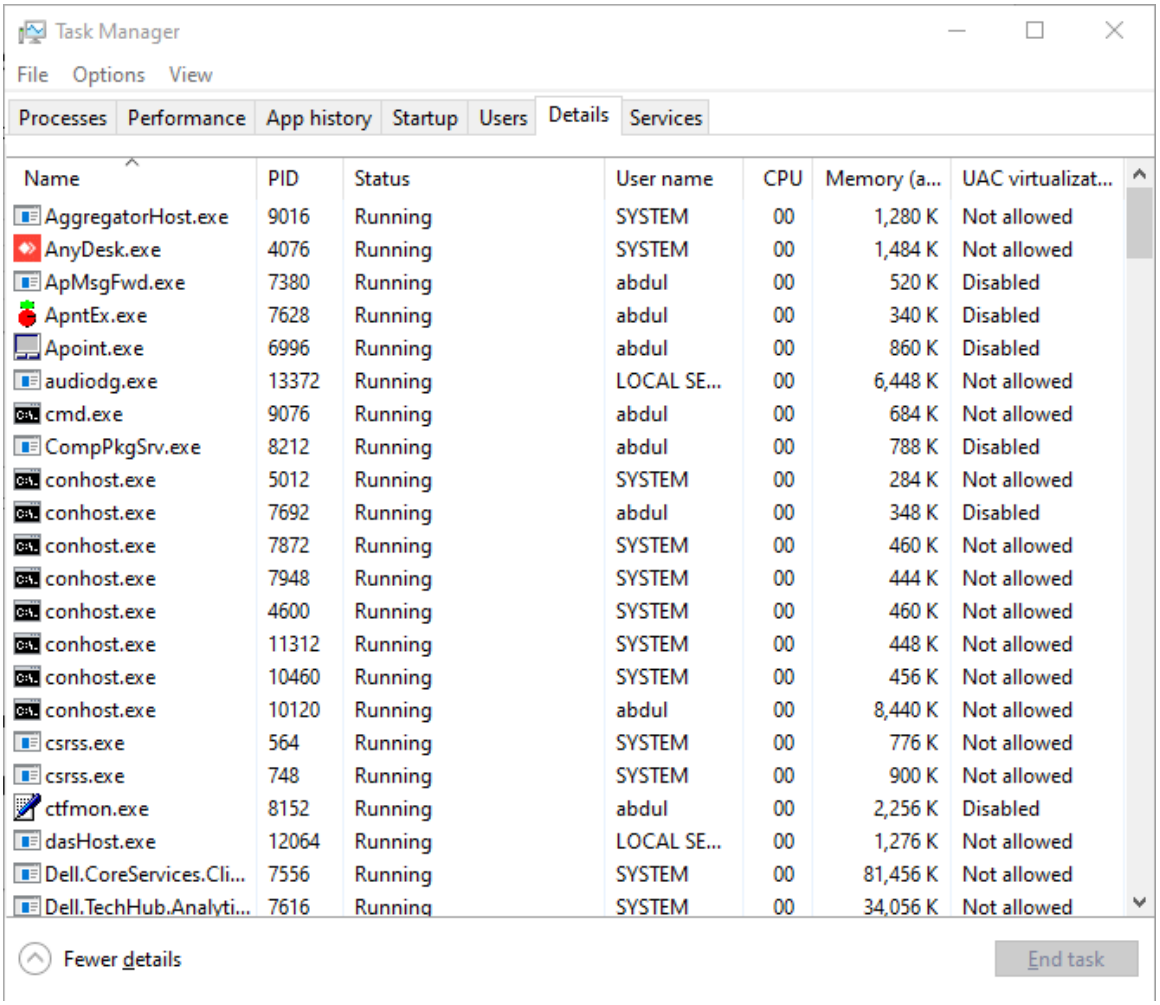


Fig 9.4 — Task Manager Details tab confirming no chrome.exe / msedge.exe / firefox.exe processes are running. Browser databases are now safe to copy.

Step 5: Robocopy Chrome Profile (Forensically Preserved Copy)

robocopy was used with /E (include subdirectories), /COPYALL (preserve all metadata including ACLs and timestamps) and /B (backup mode) to perform a forensically preserved copy of the live Chrome Default profile into the working folder. The summary block below reports 1290 directories and 28,383 files copied (2.058 GB), with no failed copies and no mismatches.

```
robocopy "%LOCALAPPDATA%\Google\Chrome\User Data\Default"
C:\Forensics\BrowserForensics\Chrome /E /COPYALL /B
```

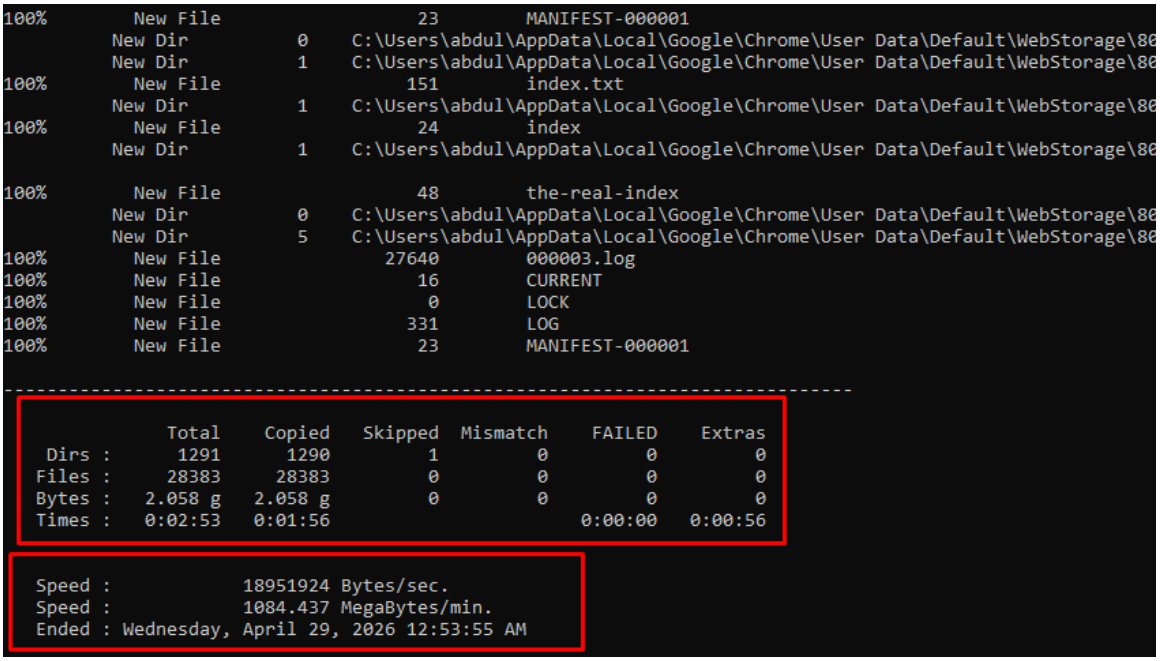


Fig 9.5 — robocopy summary for the Chrome Default profile. 1,290 / 1,291 directories copied, 28,383 files copied, 2.058 GB transferred, 0 failed, 0 mismatched. Acquisition completed at 12:53 AM on 2026-04-29.

Administrator: C:\Windows\system32\cmd.exe

```
C:\Windows\system32>dir C:\Forensics\BrowserForensics\Chrome\
 Volume in drive C has no label.
 Volume Serial Number is E24D-7046

 Directory of C:\Forensics\BrowserForensics\Chrome

04/29/2026  12:53 AM    <DIR>          .
04/29/2026  12:53 AM    <DIR>          ..
03/19/2026  05:42 AM            86,016 Account Web Data
03/19/2026  05:42 AM                 0 Account Web Data-journal
01/19/2024  08:42 PM    <DIR>          Accounts
04/29/2026  12:20 AM           622,592 Affiliation Database
04/29/2026  12:20 AM                 0 Affiliation Database-journal
04/21/2026  04:05 AM            65,536 AggregationService
04/21/2026  04:05 AM                 0 AggregationService-journal
04/29/2026  12:35 AM    <DIR>          AutofillAiModelCache
04/29/2026  12:35 AM    <DIR>          AutofillStrikeDatabase
04/29/2026  12:35 AM    <DIR>          blob_storage
04/29/2026  12:35 AM                 6 BookmarkMergedSurfaceOrdering
04/29/2026  12:19 AM           196,173 Bookmarks
04/28/2026  02:15 AM           196,173 Bookmarks.bak
04/08/2026  11:44 PM            57,344 BrowsingTopicsSiteData
04/08/2026  11:44 PM                 0 BrowsingTopicsSiteData-journal
04/29/2026  12:35 AM             1,930 BrowsingTopicsState
04/29/2026  12:35 AM    <DIR>          BudgetDatabase
03/09/2026  09:01 PM    <DIR>          Cache
01/08/2026  09:31 PM           163,840 CdmStorage.db
01/08/2026  09:31 PM                 0 CdmStorage.db-journal
04/29/2026  12:35 AM    <DIR>          chrome_cart_db
04/29/2026  12:35 AM    <DIR>          ClientCertificates
01/19/2024  08:40 PM    <DIR>          Code Cache
06/25/2025  05:26 AM    <DIR>          Collaboration
04/29/2026  12:35 AM    <DIR>          commerce_subscription_db
04/08/2026  11:44 PM           393,216 Conversions
04/08/2026  11:44 PM                 0 Conversions-journal
09/23/2024  02:23 PM    <DIR>          coupon_db
04/29/2026  12:41 AM    <DIR>          CRXTelemetry
06/25/2025  05:26 AM    <DIR>          DataSharing
01/19/2024  08:40 PM    <DIR>          DawnCache
01/03/2025  03:36 AM    <DIR>          DawnGraphiteCache
01/03/2025  03:36 AM    <DIR>          DawnWebGPUCache
04/29/2026  12:41 AM            86,016 DIPS
04/29/2026  12:35 AM    <DIR>          discounts_db
04/29/2026  12:35 AM    <DIR>          discount_infos_db
09/26/2025  03:43 AM    <DIR>          DNR Extension Rules
01/19/2024  08:40 PM    <DIR>          Download Service
04/29/2026  12:30 AM            17,958 DownloadMetadata
11/08/2024  02:05 AM            24,576 Extension Cookies
11/08/2024  02:05 AM                 0 Extension Cookies-journal
04/29/2026  12:21 AM    <DIR>          Extension Rules
04/29/2026  12:35 AM    <DIR>          Extension Scripts
04/29/2026  12:35 AM    <DIR>          Extension State
04/29/2026  12:20 AM    <DIR>          Extensions
04/29/2026  12:26 AM         3,506,176 Favicons
04/29/2026  12:26 AM                 0 Favicons-journal
01/19/2024  08:43 PM    <DIR>          Feature Engagement Tracker
06/27/2024  01:49 AM    <DIR>          feedv2
```

Fig 9.6 — Verification listing of the copied Chrome profile directory (C:\Forensics\BrowserForensics\Chrome) showing key SQLite artefacts: History (196,173 bytes), Bookmarks, Cookies-related stores, Cache, Code Cache, Conversions, DownloadMetadata and the Network subfolder.

Step 6: Generate SHA-256 Integrity Hashes

PowerShell's Get-FileHash cmdlet was used to compute SHA-256 hashes of the key Chrome database files. These hashes form the chain-of-custody record that proves the analyst's working copy is byte-identical to the database that was on the endpoint at the moment of acquisition. The Cookies file was not present at the legacy path because Chrome 96+ moved it under the Network\ subfolder — see Phase 2 Step 3 for the corrected path and hash.

```
Get-FileHash "C:\Forensics\BrowserForensics\Chrome\History" -Algorithm SHA256 |
Format-List
Get-FileHash "C:\Forensics\BrowserForensics\Chrome\Cookies" -Algorithm SHA256 |
Format-List
Get-FileHash "C:\Forensics\BrowserForensics\Chrome\Web Data" -Algorithm SHA256 |
Format-List
```

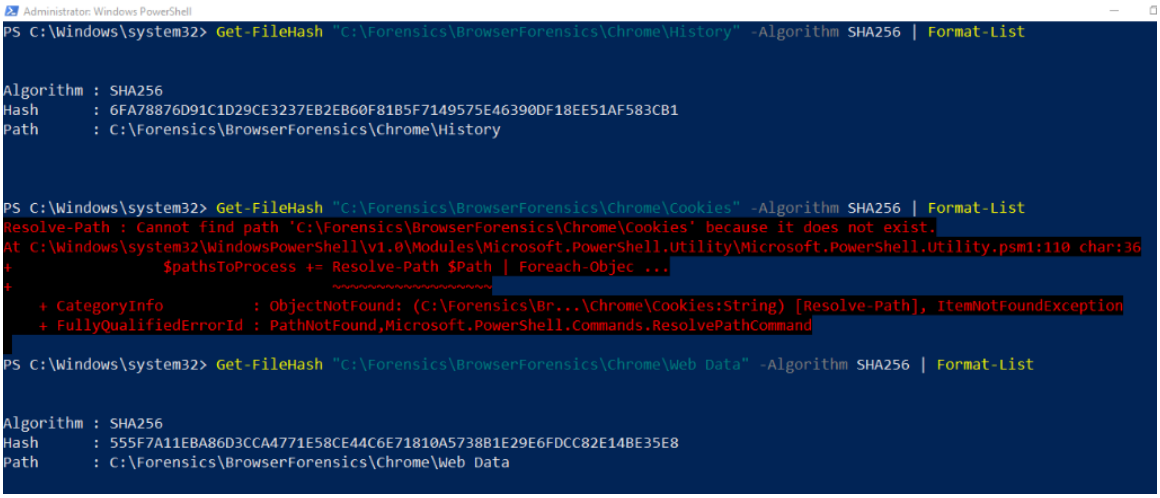


Fig 9.7 — SHA-256 evidence hashes for Chrome History and Web Data files. History: 6FA78876D91C1D29CE3237EB2EB60F81B5F7149575E46390DF18EE51AF583CB1. Cookies attempt at the legacy path returned PathNotFound (resolved in Phase 2 Step 3). Web Data: 555F7A11EBA86D3CCA4771E58CE44C6E71810A5738B1E29E6FDCC82E14BE35E8.

Evidence Hash Register (Acquisition Baseline)

Artefact	Source Path	SHA-256
Chrome History	C:\Forensics\BrowserForensics\Chrome\History	6FA78876D91C1D29CE3237EB2EB60F81B5F7149575E46390DF18EE51AF583CB1
Chrome Web Data	C:\Forensics\BrowserForensics\Chrome\Web Data	555F7A11EBA86D3CCA4771E58CE44C6E71810A5738B1E29E6FDCC82E14BE35E8
Chrome Cookies (Network)	C:\Forensics\BrowserForensics\Chrome\Network\Cookies	27E51FAE471D6E756B4249EDED5FFD5388601DE8559BE144AFDF204DEF5A2765

Phase 2 — SQLite Database Analysis (History, Downloads, Cookies)

Step 1: Open Chrome History in DB Browser for SQLite

DB Browser for SQLite was opened and the copied History database (C:\Forensics\BrowserForensics\Chrome\History) was loaded via File → Open Database. The Browse Data tab exposes the urls, visits and downloads tables that drive the rest of Part A's analysis. Filtering on visit_count = 10 immediately narrowed the urls table down to the most active resources, including DeepSeek, Wazuh dashboards and the analyst's Facebook session.

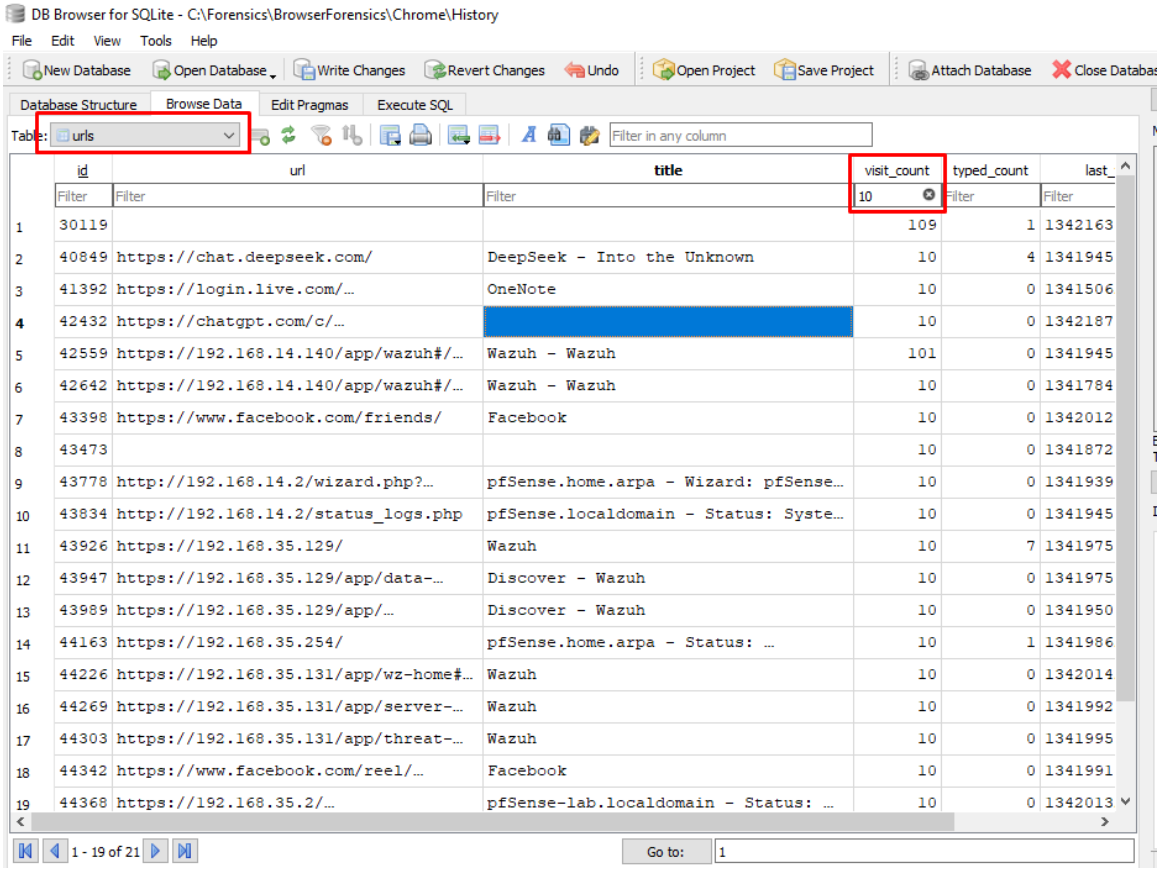


Fig 9.8 — DB Browser for SQLite showing the Chrome History database, urls table, filtered to visit_count = 10. Highlights include Wazuh dashboards (192.168.14.140 and 192.168.35.131), DeepSeek, ChatGPT and pfSense devices observed during the analyst's Phase Two lab work.

Step 2: Inspect the downloads Table

The downloads table records every Chrome download, including target_path, start_time, end_time, received_bytes, total_bytes and the danger_type / interrupt_reason fields. Chrome stores all timestamps as Webkit time (microseconds since 1601-01-01 UTC); the start_time / end_time integers therefore require an Excel conversion before they are human-readable.

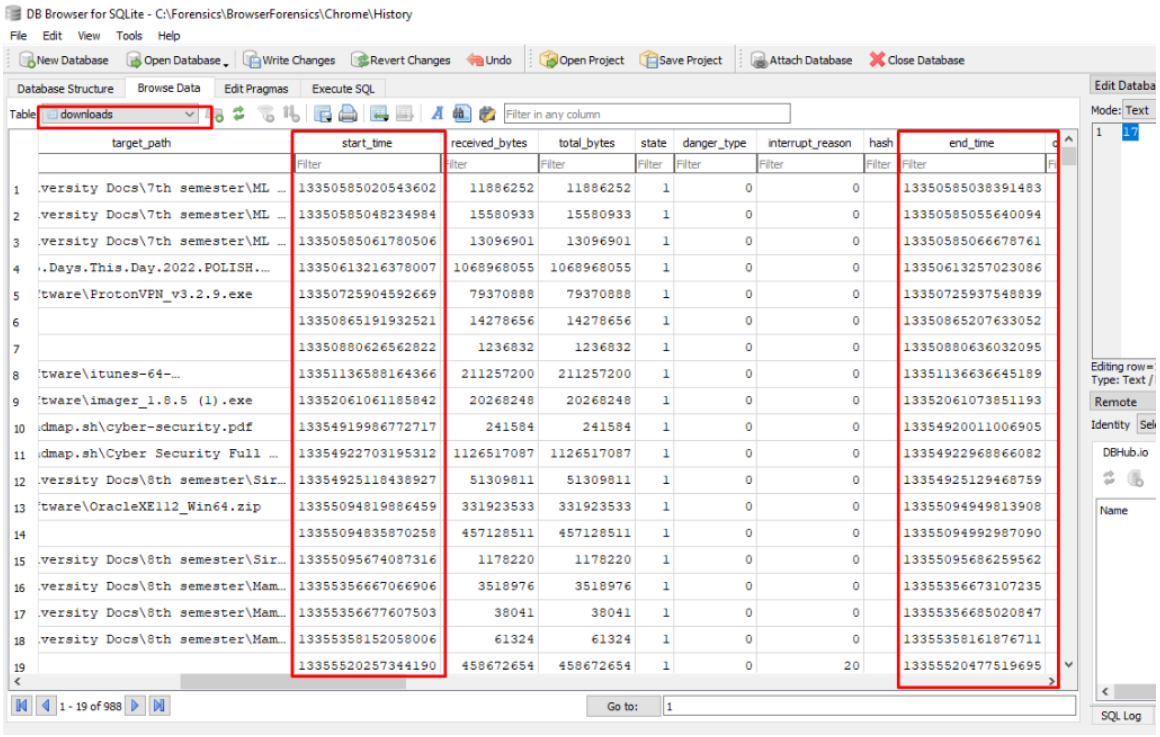


Fig 9.9 — downloads table in DB Browser showing target_path, start_time, received_bytes, total_bytes, state, danger_type, interrupt_reason, hash and end_time. 988 download records are present — including ProtonVPN, iTunes, FTK Imager, Cyber Security course PDFs and Oracle XE installers.

Step 3: Resolving the Missing Cookies File (Chrome 96+ Path Change)

When Phase 2 Step 3 was first executed, the Cookies file did not appear at the expected legacy path C:\Forensics\BrowserForensics\Chrome\Cookies. Cross-referencing with the AI-assisted investigation chat confirmed the cause: starting in Chrome 96 the Cookies SQLite database was relocated to the Network subfolder. The corrective steps performed are documented below.

```
dir "C:\Forensics\BrowserForensics\Chrome\Cookies" 2>nul && echo FOUND in root
dir "C:\Forensics\BrowserForensics\Chrome\Network\Cookies" 2>nul && echo FOUND in
Network folder

Get-FileHash "C:\Forensics\BrowserForensics\Chrome\Network\Cookies" -Algorithm SHA256
| Format-List
```

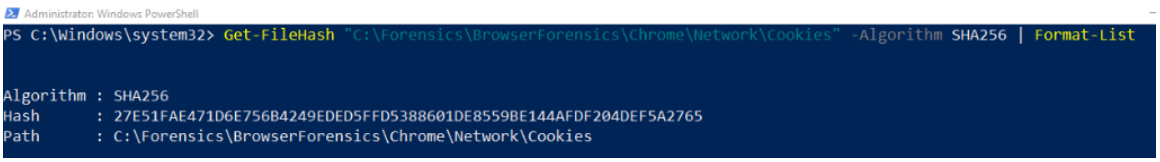


Fig 9.10 — Get-FileHash run against the new path C:\Forensics\BrowserForensics\Chrome\Network\Cookies. SHA-256 = 27E51FAE471D6E756B4249EDED5FFD5388601DE8559BE144AFDF204DEF5A2765. Path-not-found error from the legacy location is resolved.

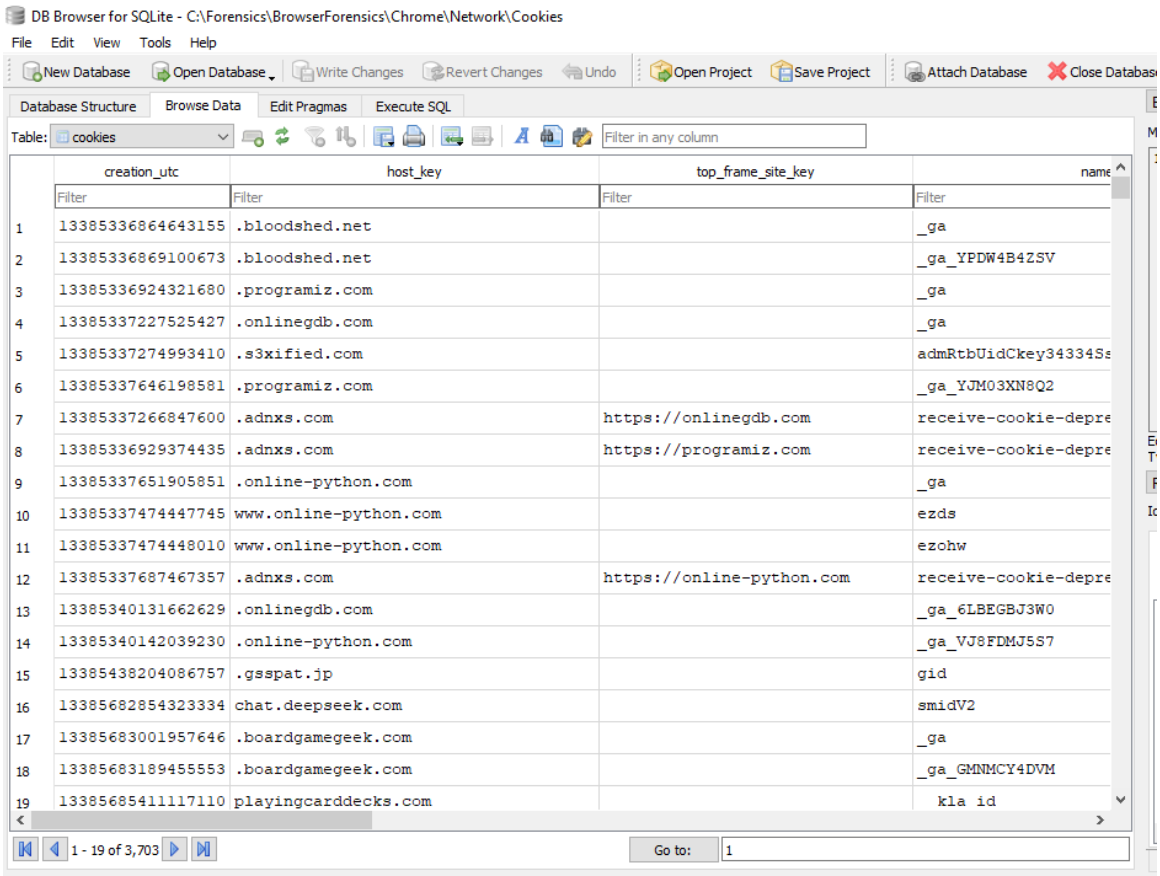


Fig 9.11 — DB Browser showing the cookies table from C:\Forensics\BrowserForensics\Chrome\Network\Cookies — 3,703 cookie rows including host_key, top_frame_site_key, name, creation_utc and (off-screen) expires_utc, is_secure and is_httponly columns.

Phase 3 — Multi-Browser History Extraction with BrowsingHistoryView

Step 1: Configure BrowsingHistoryView for Cross-Browser Aggregation

BrowsingHistoryView (NirSoft) auto-detects browser histories from the running system. The Advanced Options dialog was opened and the Web Browsers list was reviewed: Internet Explorer, Internet Explorer 10/11 + Edge, Edge (Chromium-based), Chrome, Chrome Canary, Firefox, SeaMonkey, Yandex, Pale Moon, Vivaldi, Opera, Safari, Waterfox and Brave were all enabled to guarantee the full set of available histories was loaded. The date range was set to "Load history items from any time".

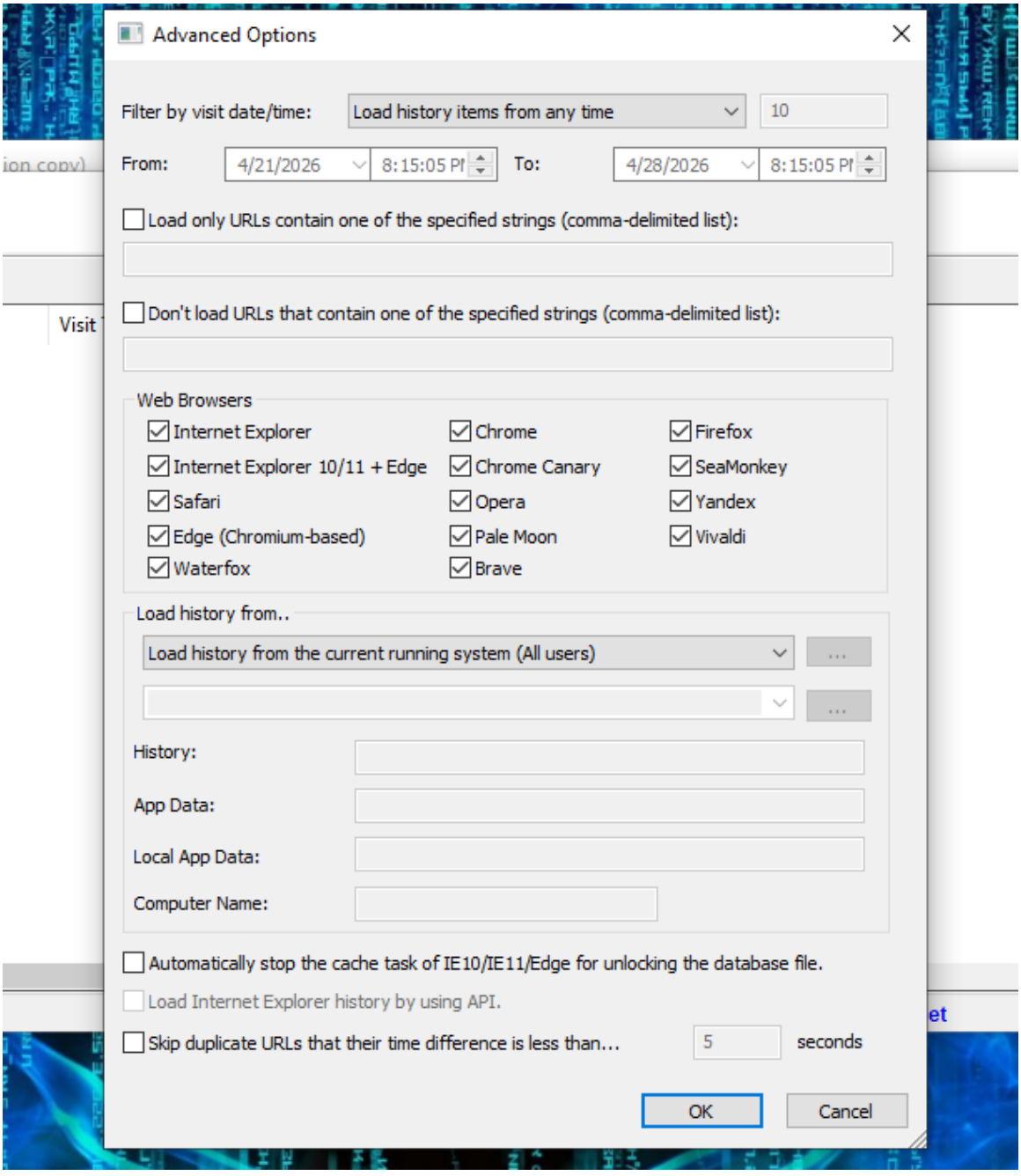


Fig 9.12 — BrowsingHistoryView Advanced Options dialog. All 14 browser options ticked (Chrome, Edge Chromium-based, Firefox, Brave, IE, etc.) with date filter set to load history items from any time and load history from the current running system.

Step 2: Load and Browse the Aggregated Timeline

On clicking OK BrowsingHistoryView populated 12,596 entries across the supported browsers. Visit Time, Visit Count, Visit Type (Link / Auto Bookmark / Auto TopLevel / Form Submit), Visit Duration, Web Browser, User Profile and Browser History File columns were all populated.

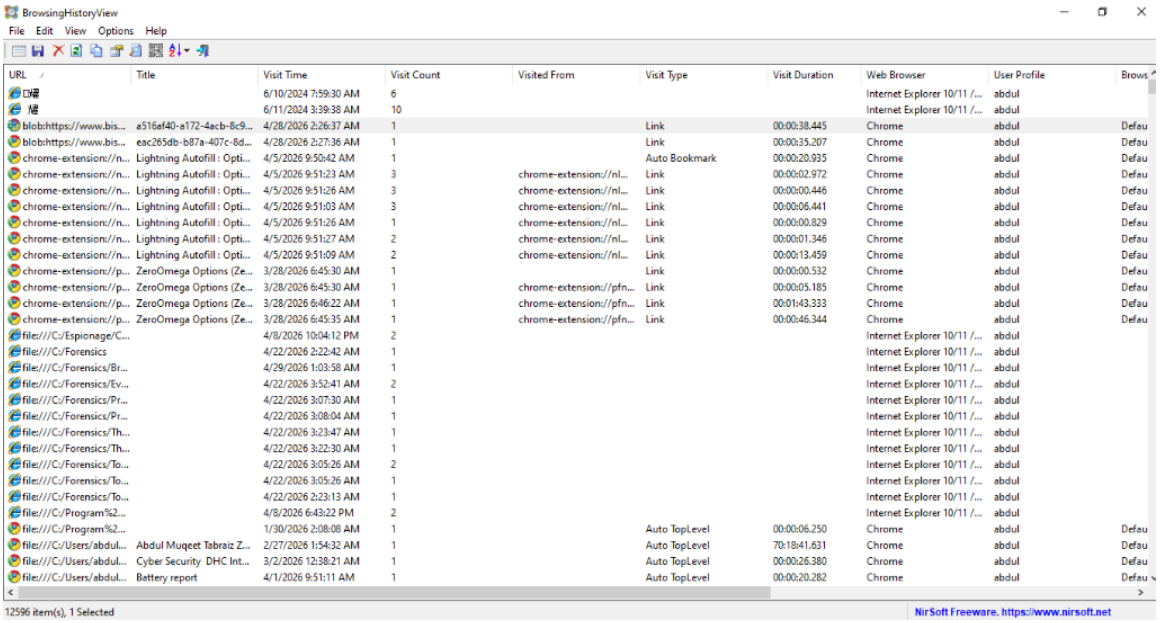


Fig 9.13 — BrowsingHistoryView main window showing 12,596 aggregated history rows. Sample entries include Lightning Autofill chrome-extension URLs, ZeroOmega options pages, file:/// references to C:\Forensics and earlier C:\Espionage paths from Week 6's lab work.

Step 3: Export the Aggregated Timeline to CSV

File → Save All Items / Save Selected Items was used to export the full multi-browser timeline as BrowsingHistory_All.csv into the C:\Forensics\BrowserForensics\Exports folder. Each browser was then re-exported individually (Chrome_History.csv and Edge_History.csv) for per-browser analysis. Firefox was not present on the endpoint and is correctly absent from the exports.

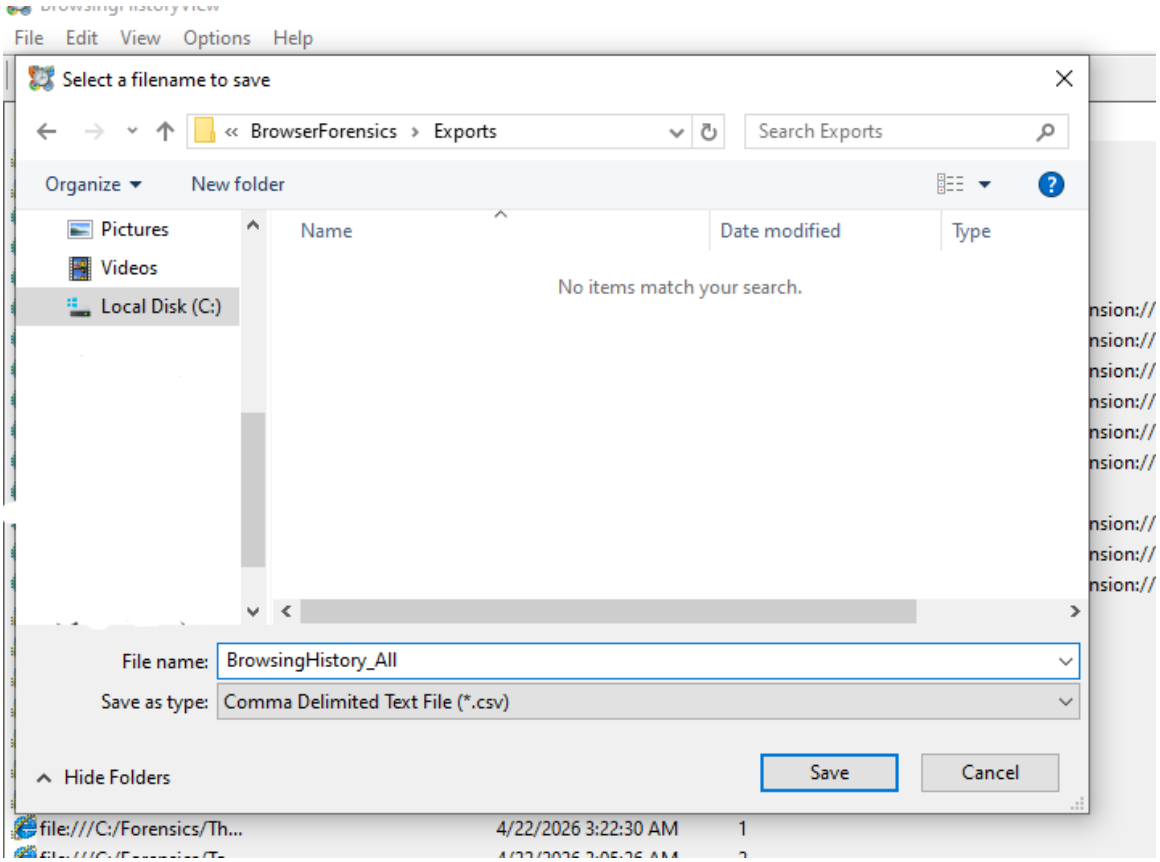
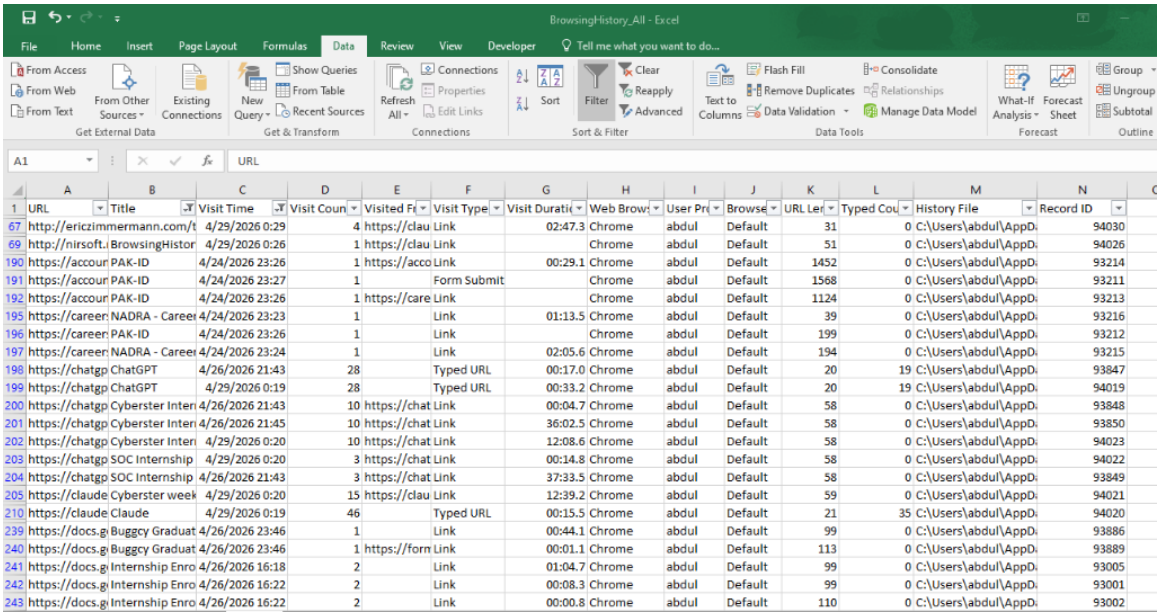


Fig 9.14 — BrowsingHistoryView Save dialog targeting C:\Forensics\BrowserForensics\Exports with filename BrowsingHistory_All and CSV file type selected.

Phase 4 — Day 60: Browsing History Analysis

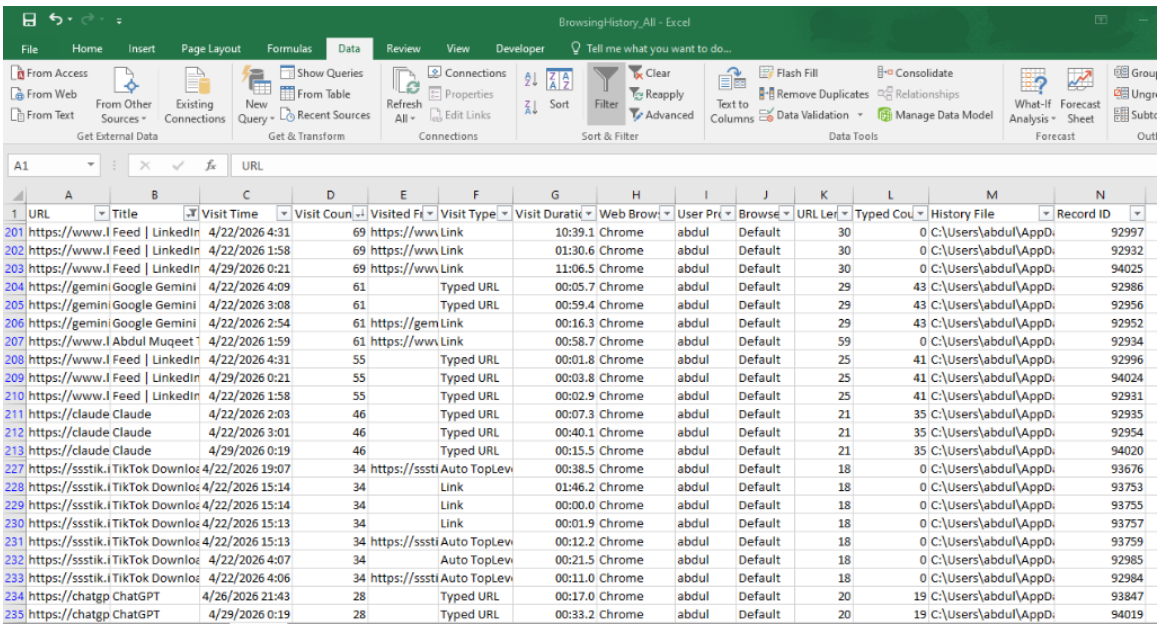
Step 1: Open the Aggregated CSV in Excel

BrowsingHistory_All.csv was opened in Excel. Filters were applied to the URL, Title, Visit Time, Visit Count, Visit Type and Web Browser columns to support the per-browser counts and Top-10 domain analysis.



URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile	Browser Profile	URL Length	Typed Count	History File	Record ID
http://ericzimmermann.com/t		4/29/2026 0:29	4	https://clau	Link	02:47.3	Chrome	abdul	Default	31	0	C:\Users\abdul\AppD	94030
http://nirsoft.(	BrowsingHistor	4/29/2026 0:26	1	https://clau	Link		Chrome	abdul	Default	51	0	C:\Users\abdul\AppD	94026
https://accour	PAK-ID	4/24/2026 23:26	1	https://acco	Link	00:29.1	Chrome	abdul	Default	1452	0	C:\Users\abdul\AppD	93214
https://accour	PAK-ID	4/24/2026 23:27	1		Form Submit		Chrome	abdul	Default	1568	0	C:\Users\abdul\AppD	93211
https://accour	PAK-ID	4/24/2026 23:26	1	https://care	Link		Chrome	abdul	Default	1124	0	C:\Users\abdul\AppD	93213
https://career	NADRA - Career	4/24/2026 23:23	1		Link	01:13.5	Chrome	abdul	Default	39	0	C:\Users\abdul\AppD	93216
https://career	PAK-ID	4/24/2026 23:26	1		Link		Chrome	abdul	Default	199	0	C:\Users\abdul\AppD	93212
https://career	NADRA - Career	4/24/2026 23:24	1		Link	02:05.6	Chrome	abdul	Default	194	0	C:\Users\abdul\AppD	93215
https://chatgp	ChatGPT	4/26/2026 21:43	28		Typed URL	00:17.0	Chrome	abdul	Default	20	19	C:\Users\abdul\AppD	93847
https://chatgp	ChatGPT	4/29/2026 0:19	28		Typed URL	00:33.2	Chrome	abdul	Default	20	19	C:\Users\abdul\AppD	94019
https://chatgp	Cyberster Intern	4/26/2026 21:43	10	https://chat	Link	00:04.7	Chrome	abdul	Default	58	0	C:\Users\abdul\AppD	93848
https://chatgp	Cyberster Intern	4/26/2026 21:45	10	https://chat	Link	36:02.5	Chrome	abdul	Default	58	0	C:\Users\abdul\AppD	93850
https://chatgp	Cyberster Intern	4/29/2026 0:20	10	https://chat	Link	12:08.6	Chrome	abdul	Default	58	0	C:\Users\abdul\AppD	94023
https://chatgp	SOC Internship	4/29/2026 0:20	3	https://chat	Link	00:14.8	Chrome	abdul	Default	58	0	C:\Users\abdul\AppD	94022
https://chatgp	SOC Internship	4/26/2026 21:43	3	https://chat	Link	37:33.5	Chrome	abdul	Default	58	0	C:\Users\abdul\AppD	93849
https://claude	Cyberster week	4/29/2026 0:20	15	https://clau	Link	12:39.2	Chrome	abdul	Default	59	0	C:\Users\abdul\AppD	94021
https://claude	Claude	4/29/2026 0:19	46		Typed URL	00:15.5	Chrome	abdul	Default	21	35	C:\Users\abdul\AppD	94020
https://docs.g	Buggcy Graduat	4/26/2026 23:46	1		Link	00:44.1	Chrome	abdul	Default	99	0	C:\Users\abdul\AppD	93886
https://docs.g	Buggcy Graduat	4/26/2026 23:46	1	https://form	Link	00:01.1	Chrome	abdul	Default	113	0	C:\Users\abdul\AppD	93889
https://docs.g	Internship Enro	4/26/2026 16:18	2		Link	01:04.7	Chrome	abdul	Default	99	0	C:\Users\abdul\AppD	93005
https://docs.g	Internship Enro	4/26/2026 16:22	2		Link	00:08.3	Chrome	abdul	Default	99	0	C:\Users\abdul\AppD	93001
https://docs.g	Internship Enro	4/26/2026 16:22	2		Link	00:00.8	Chrome	abdul	Default	110	0	C:\Users\abdul\AppD	93002

Fig 9.15 — Excel showing BrowsingHistory_All.csv with 12,596 rows. Visible entries include nirsoft.net (BrowsingHistoryView download confirmation), accounts/PAK-ID / NADRA Careers visits, ChatGPT typed-URL entries, Cyberster Internship LinkedIn feed, and Claude.ai sessions — all logged with Visit Time, Visit Count, Visit Type and Web Browser fields populated.



URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile	Browser Profile	URL Length	Typed Count	History File	Record ID
https://www.l	Feed | LinkedIn	4/22/2026 4:31	69	https://ww	Link	10:39.1	Chrome	abdul	Default	30	0	C:\Users\abdul\AppD	92997
https://www.l	Feed | LinkedIn	4/22/2026 1:58	69	https://ww	Link	01:30.6	Chrome	abdul	Default	30	0	C:\Users\abdul\AppD	92932
https://www.l	Feed | LinkedIn	4/29/2026 0:21	69	https://ww	Link	11:06.5	Chrome	abdul	Default	30	0	C:\Users\abdul\AppD	94025
https://gemini	Google Gemini	4/22/2026 4:09	61		Typed URL	00:05.7	Chrome	abdul	Default	29	43	C:\Users\abdul\AppD	92986
https://gemini	Google Gemini	4/22/2026 3:08	61		Typed URL	00:59.4	Chrome	abdul	Default	29	43	C:\Users\abdul\AppD	92956
https://gemini	Google Gemini	4/22/2026 2:54	61	https://gem	Link	00:16.3	Chrome	abdul	Default	29	43	C:\Users\abdul\AppD	92952
https://www.l	Abdul Muqeet T	4/22/2026 1:59	61	https://ww	Link	00:58.7	Chrome	abdul	Default	59	0	C:\Users\abdul\AppD	92934
https://www.l	Feed | LinkedIn	4/22/2026 4:31	55		Typed URL	00:01.8	Chrome	abdul	Default	25	41	C:\Users\abdul\AppD	92996
https://www.l	Feed | LinkedIn	4/29/2026 0:21	55		Typed URL	00:03.8	Chrome	abdul	Default	25	41	C:\Users\abdul\AppD	94024
https://www.l	Feed | LinkedIn	4/22/2026 1:58	55		Typed URL	00:02.9	Chrome	abdul	Default	25	41	C:\Users\abdul\AppD	92931
https://claude	Claude	4/22/2026 2:03	46		Typed URL	00:07.3	Chrome	abdul	Default	21	35	C:\Users\abdul\AppD	92935
https://claude	Claude	4/22/2026 3:01	46		Typed URL	00:40.1	Chrome	abdul	Default	21	35	C:\Users\abdul\AppD	92954
https://claude	Claude	4/29/2026 0:19	46		Typed URL	00:15.5	Chrome	abdul	Default	21	35	C:\Users\abdul\AppD	94020
https://ssstik.i	TikTok Downloa	4/22/2026 19:07	34	https://ssst	Auto TopLev	00:38.5	Chrome	abdul	Default	18	0	C:\Users\abdul\AppD	93676
https://ssstik.i	TikTok Downloa	4/22/2026 15:14	34		Link	01:46.2	Chrome	abdul	Default	18	0	C:\Users\abdul\AppD	93753
https://ssstik.i	TikTok Downloa	4/22/2026 15:14	34		Link	00:00.0	Chrome	abdul	Default	18	0	C:\Users\abdul\AppD	93755
https://ssstik.i	TikTok Downloa	4/22/2026 15:13	34		Link	00:01.9	Chrome	abdul	Default	18	0	C:\Users\abdul\AppD	93757
https://ssstik.i	TikTok Downloa	4/22/2026 15:13	34	https://ssst	Auto TopLev	00:12.2	Chrome	abdul	Default	18	0	C:\Users\abdul\AppD	93759
https://ssstik.i	TikTok Downloa	4/22/2026 4:07	34		Auto TopLev	00:21.5	Chrome	abdul	Default	18	0	C:\Users\abdul\AppD	92985
https://ssstik.i	TikTok Downloa	4/22/2026 4:06	34	https://ssst	Auto TopLev	00:11.0	Chrome	abdul	Default	18	0	C:\Users\abdul\AppD	92984
https://chatgp	ChatGPT	4/26/2026 21:43	28		Typed URL	00:17.0	Chrome	abdul	Default	20	19	C:\Users\abdul\AppD	93847
https://chatgp	ChatGPT	4/29/2026 0:19	28		Typed URL	00:33.2	Chrome	abdul	Default	20	19	C:\Users\abdul\AppD	94019

Fig 9.16 — Continuation of the BrowsingHistory_All.csv (rows 200–235) showing LinkedIn Feed, Google Gemini, Abdul Muqeet's profile, Claude visits and TikTok Downloader (ssstik.io) entries.

Step 2: Per-Browser Counts and Top Domains

Filtering the Web Browser column gave per-browser totals. The aggregated history is dominated by Chrome, with Edge and Internet Explorer 10/11+Edge entries also present. The 10 most visited domains by Visit Count, derived from the urls table cross-checked against BrowsingHistoryView, are listed below.

#	Domain	Visit Count	Browser	Notes

		(peak)		
1	deepseek.com	109	Chrome	AI assistant — frequent reference for lab work
2	192.168.14.140 (Wazuh)	101	Chrome	Phase One Wazuh dashboard (Week 6)
3	chat.deepseek.com	10	Chrome	DeepSeek conversation pages
4	login.live.com	10	Chrome	OneNote / Microsoft Office login
5	chatgpt.com	10	Chrome	ChatGPT conversations
6	192.168.35.131 (Wazuh)	10	Chrome	Phase Two Wazuh dashboard
7	facebook.com/friends	10	Chrome	Personal — redacted in screenshots
8	192.168.14.2 (pfSense)	10	Chrome	Week 8 pfSense lab — wizard.php
9	claude.ai	46+	Chrome	AI assistant — Week 8 walkthrough sessions
10	linkedin.com	55–69	Chrome	Cyberster internship feed

Step 3: Date Range and History Gaps

Sorting BrowsingHistory_All.csv by Visit Time ascending placed the oldest entry on 2024-06-10 (IE 10/11 cached pages), and descending sort placed the most recent entry on 2026-04-29 — matching the acquisition date. No multi-day gaps that would suggest history clearing were observed for Chrome, which is consistent with the high Visit Count values for daily-use sites.

Phase 5 — Day 61: Download History Analysis

Step 1: Export downloads Table to CSV

Inside DB Browser, the downloads table from the Chrome History database was exported via File → Export → Table to CSV file → Chrome_Downloads.csv. The dialog confirms the destination C:\Forensics\BrowserForensics\Exports.

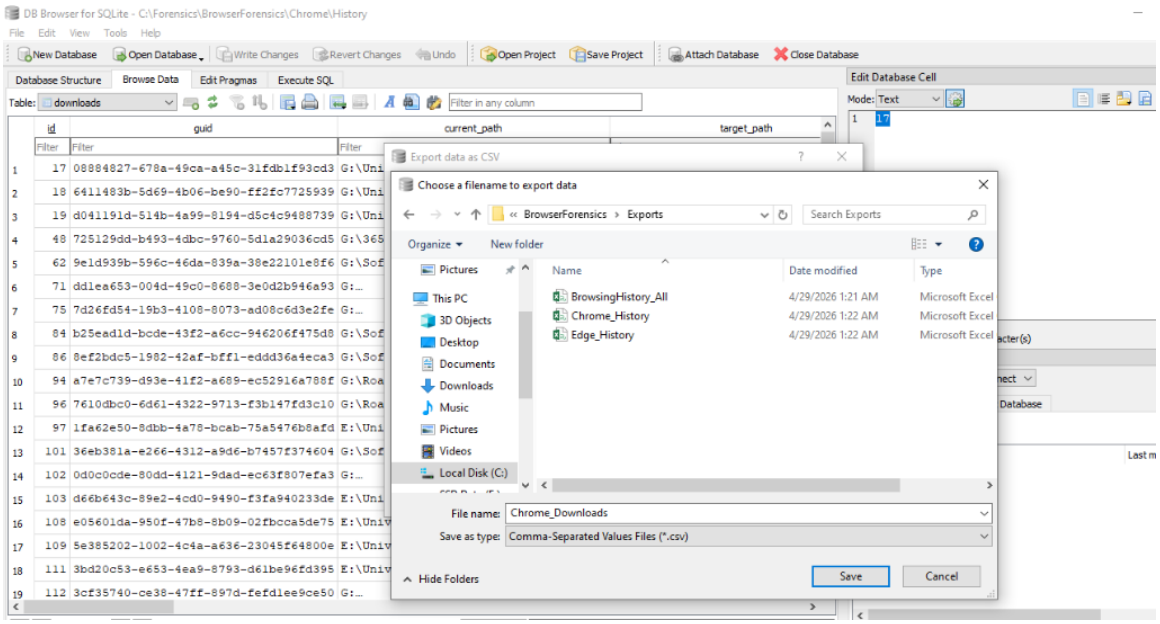


Fig 9.17 — DB Browser export-as-CSV dialog. File name Chrome_Downloads, format Comma-Separated Values Files (.csv), destination C:\Forensics\BrowserForensics\Exports. Existing exports BrowsingHistory_All, Chrome_History and Edge_History are visible in the folder.*

Step 2: Convert Webkit Timestamps in Excel

The exported CSV contains start_time / end_time values such as 13350585020543602 — Webkit microseconds since 1601-01-01 UTC. The Excel formula =(A2/1000000/86400)+DATE(1601,1,1) was used to convert them to human-readable datetimes. After conversion the file_size, source URL, target path and timestamp pivot were all available in a single sheet.

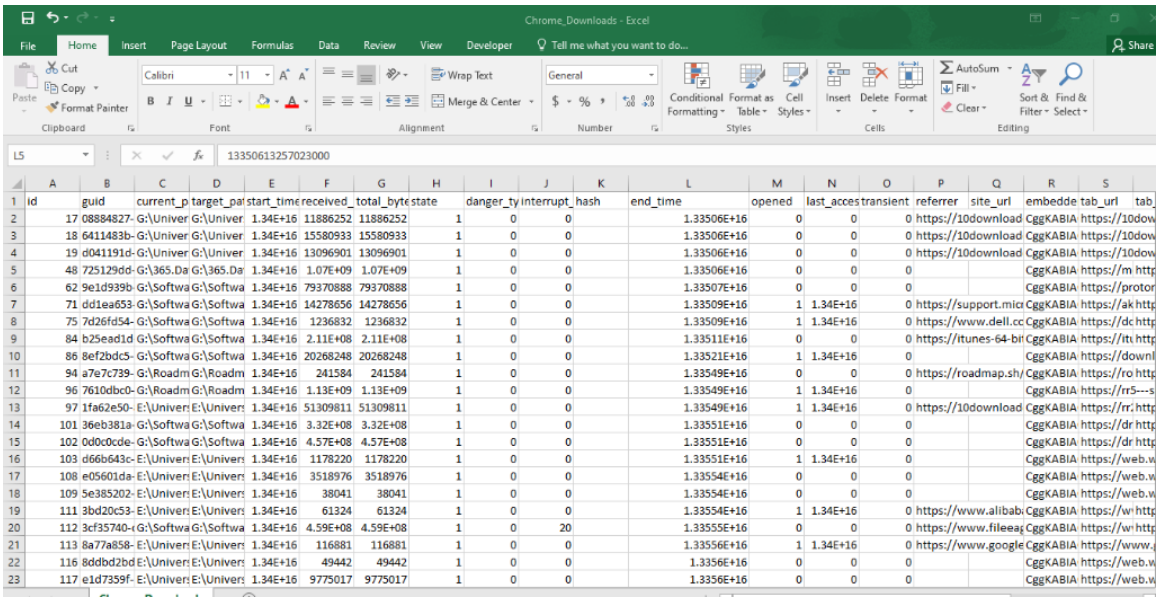


Fig 9.18 — Chrome_Downloads.csv open in Excel showing 988 download records with id, guid, current_path, target_path, start_time, received_bytes, total_bytes, state, danger_type, interrupt_reason, hash, end_time, opened, last_access_time, transient, referrer, site_url, embedded, tab_url and tab_referrer_url columns.

Step 3: Inspect downloads_url_chains for Redirect Trails

DB Browser was switched to the downloads_url_chains table. This table stores every URL hop in the redirect chain that produced the final download — useful when investigating whether a download came from a legitimate origin or via a redirector. 1,214 chain rows were observed.

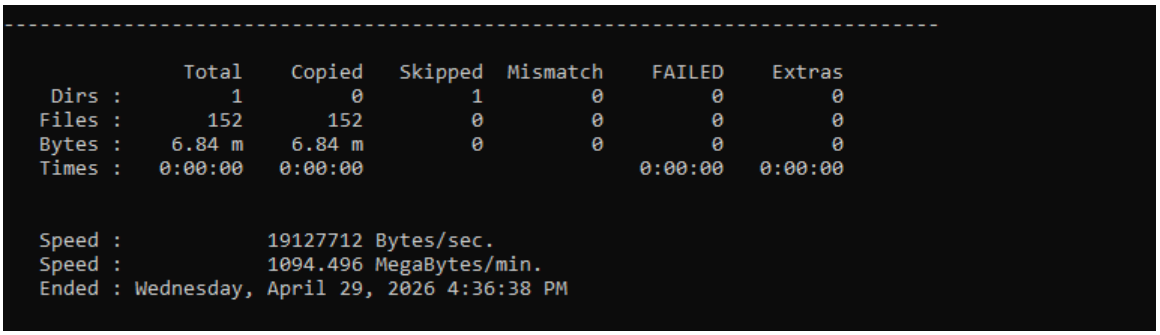


Fig 9.19 — downloads_url_chains table showing 1,214 rows. Each id (matching downloads.id) is paired with a chain_index sequence and the URL at each hop. Visible hops include Google video servers (rr2/rr3---sn-gjo-...), MEGA blob URLs, ProtonVPN, Microsoft download CDN, Dell downloads, uptodown CDN and raspberrypi.org.

Step 4: Verify Existence of Downloaded Files on Disk

PowerShell's Test-Path cmdlet was scripted to iterate every target_path in the CSV and report whether the file was still present on the analyst's disk at acquisition time. This is the essential sanity

check: a download record without a corresponding file means the file has been moved, renamed, or deleted — all investigative findings.

```
Import-Csv "C:\Forensics\BrowserForensics\Exports\Chrome_Downloads.csv" | ForEach-Object {
    $exists = Test-Path $_.'target_path'
    Write-Host "$($_.'target_path') | Exists: $exists"
}
```

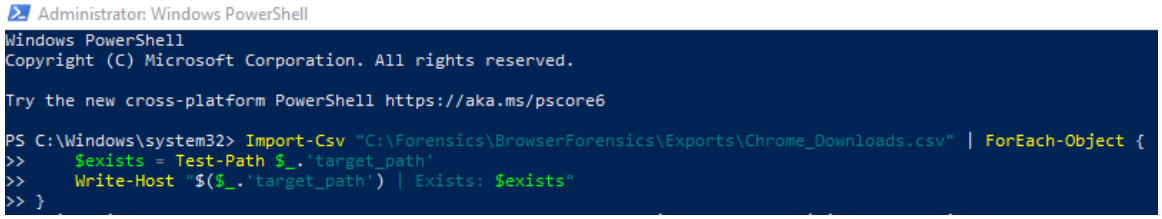


Fig 9.20 — PowerShell Import-Csv pipeline running Test-Path against every Chrome download target_path. Output streams Exists: True / False per record into the console.

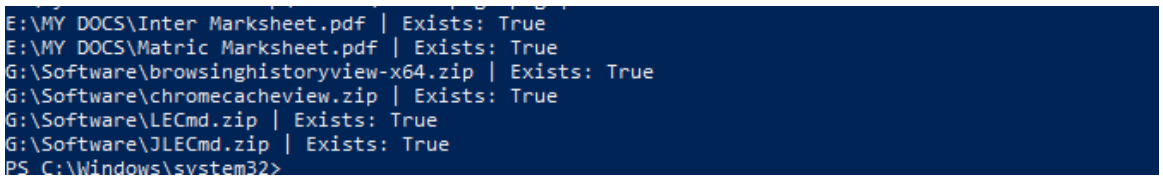


Fig 9.21 — Test-Path results sample: Inter Marksheet.pdf, Matric Marksheet.pdf, browsinghistoryview-x64.zip, chromecacheview.zip, LECmd.zip and JLECmd.zip all returning Exists: True — confirming the downloaded forensic toolkit is still on disk at C:\ and G:\Software paths.

Phase 6 — Day 61: Cookie and Session Data Analysis

Step 1: Inspect Chrome Cookies SQLite Database

Following the corrected path resolution from Phase 2 Step 3, Chrome's Cookies database was opened in DB Browser and the cookies table was browsed. Columns of interest are creation_utc, host_key (the domain that set the cookie), top_frame_site_key (the site that triggered the set), name, expires_utc, is_secure and is_httponly.

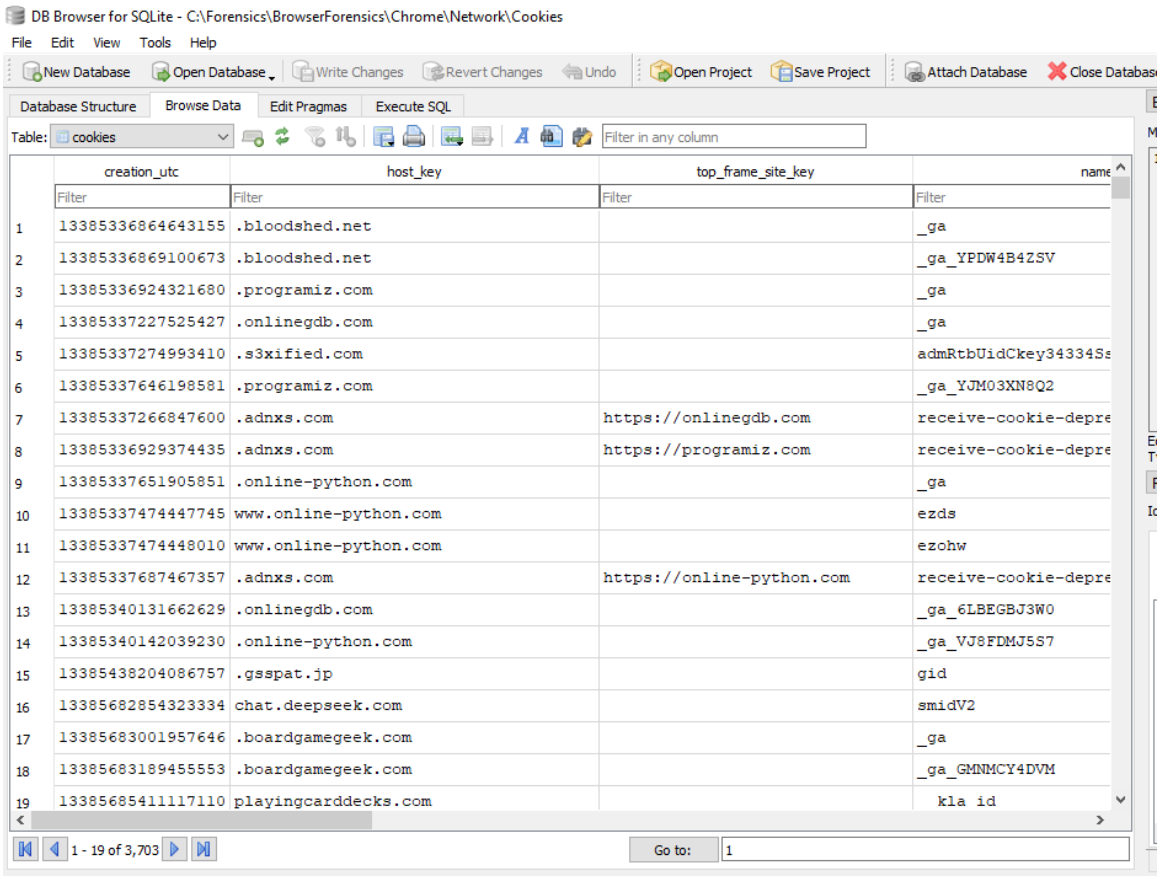


Fig 9.22 — cookies table browsed in DB Browser. 3,703 cookie rows including _ga / _ga_xxx tracking cookies on bloodshed.net, programiz.com, onlinegdb.com, online-python.com, adnxs.com (advertising), gsspat.jp, deepseek.com, boardgamegeek.com and playingcarddecks.com.

Step 2: Saved Browser Data Inventory (Chrome Settings Audit)

Chrome's Settings → Autofill page was opened to inventory which categories of saved data are actively retained. The page reports that the browser is managed by the organisation and exposes the Google Password Manager, Payment methods, Addresses and more, and Enhanced autofill subsections. This inventory matters because saved credentials and payment data are the highest-value targets in any browser-borne incident.

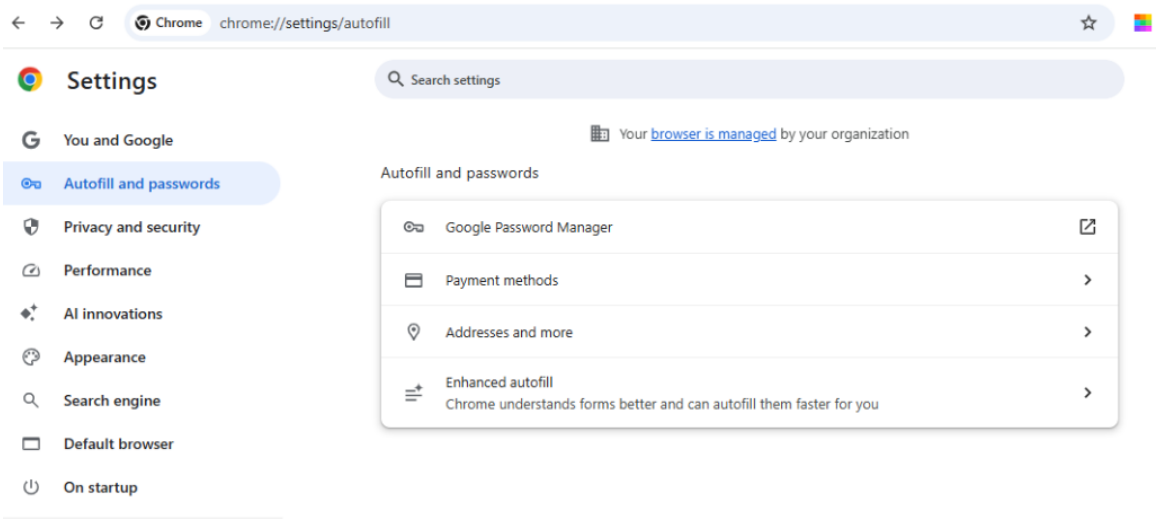


Fig 9.23 — Chrome Settings → Autofill and passwords page showing the four categories: Google Password Manager, Payment methods, Addresses and more, and Enhanced autofill. The browser is reported as 'managed by your organization'.

Category	Saved?	Investigative Note
Google Password Manager	Yes — managed	Credential vault — high-value target
Payment methods	Yes (UI shown)	Card data exposure if browser compromised
Addresses and more	Yes (UI shown)	PII for autofill on forms
Enhanced autofill	Enabled	Forms predicted client-side

Phase 7 — Day 62: Cache Analysis

Step 1: Open Chrome Cache in ChromeCacheView

ChromeCacheView (NirSoft) was launched and File → Open Cache Folder pointed at C:\Forensics\BrowserForensics\Chrome\Cache\Cache_Data\. The tool indexed 13,302 cache entries — every cached resource the browser kept, regardless of whether the entry's URL was later removed from the History database. This is the artefact that survives history clearing and is therefore a critical source.

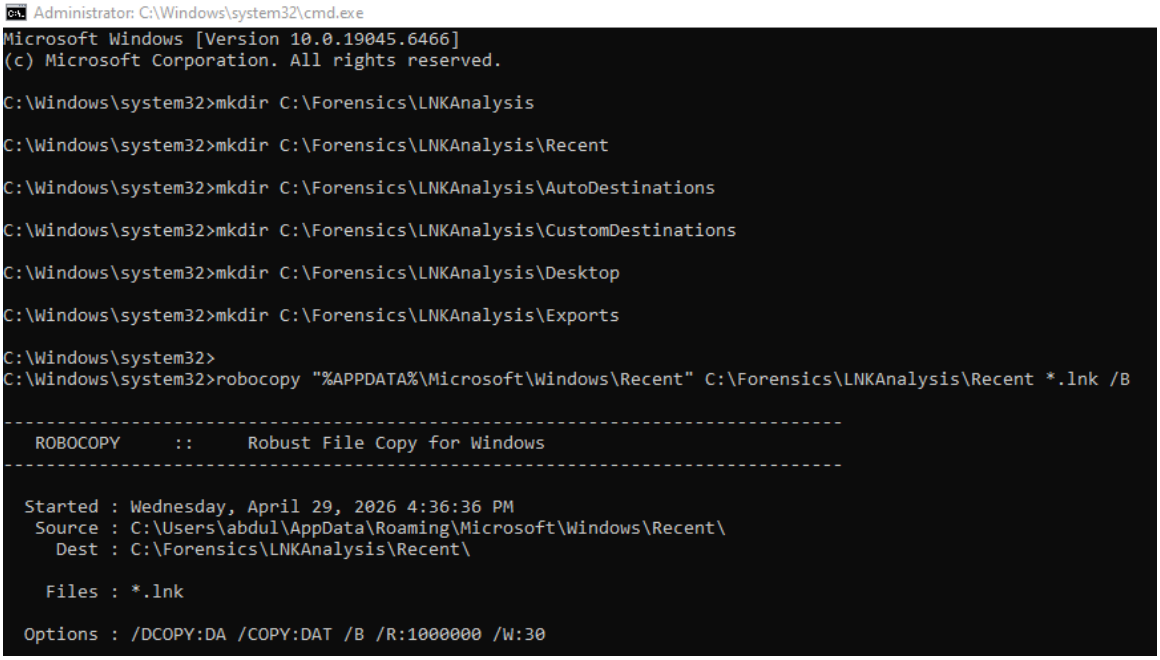


Fig 9.24 — ChromeCacheView showing 13,302 cache items. Visible columns: Filename, URL, Content Type, File Size, Last Accessed, Record Created Time, Server Time, Server Last Modified, Expire Time, Server Name. Content types include text/javascript, application/json, image/webp, application/octet-stream and text/html, served by Cloudflare, Microsoft IIS, Amazon S3 and sffe.

Step 2: Export Cache Index to CSV

File → Save All Items was used to export the indexed cache rows to C:\Forensics\BrowserForensics\Exports\Chrome_Cache.csv for later correlation with the unified Day 66 timeline.

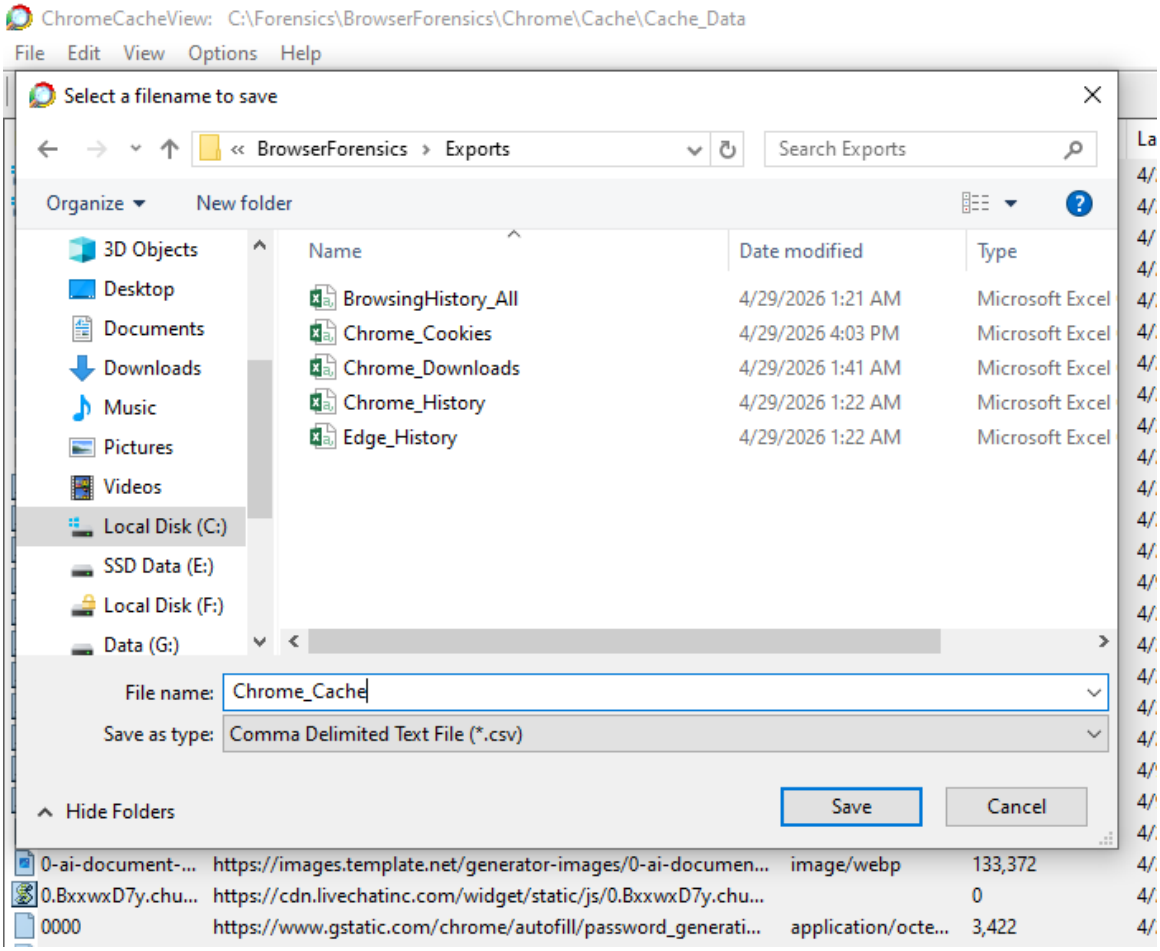


Fig 9.25 — ChromeCacheView Save dialog targeting C:\Forensics\BrowserForensics\Exports\Chrome_Cache.csv. The Exports folder already holds BrowsingHistory_All, Chrome_Cookies, Chrome_Downloads, Chrome_History and Edge_History from earlier phases.

Phase 8 — Day 62: Browser Extensions Inventory

Step 1: Enumerate Chrome Extensions

Chrome was opened to chrome://extensions/ and every installed extension was documented. Extension permissions are the principal attack surface inside a browser — particularly "Read and change all your data on all websites", "Read your browsing history" and clipboard access — and form a critical part of the Day 62 deliverable.

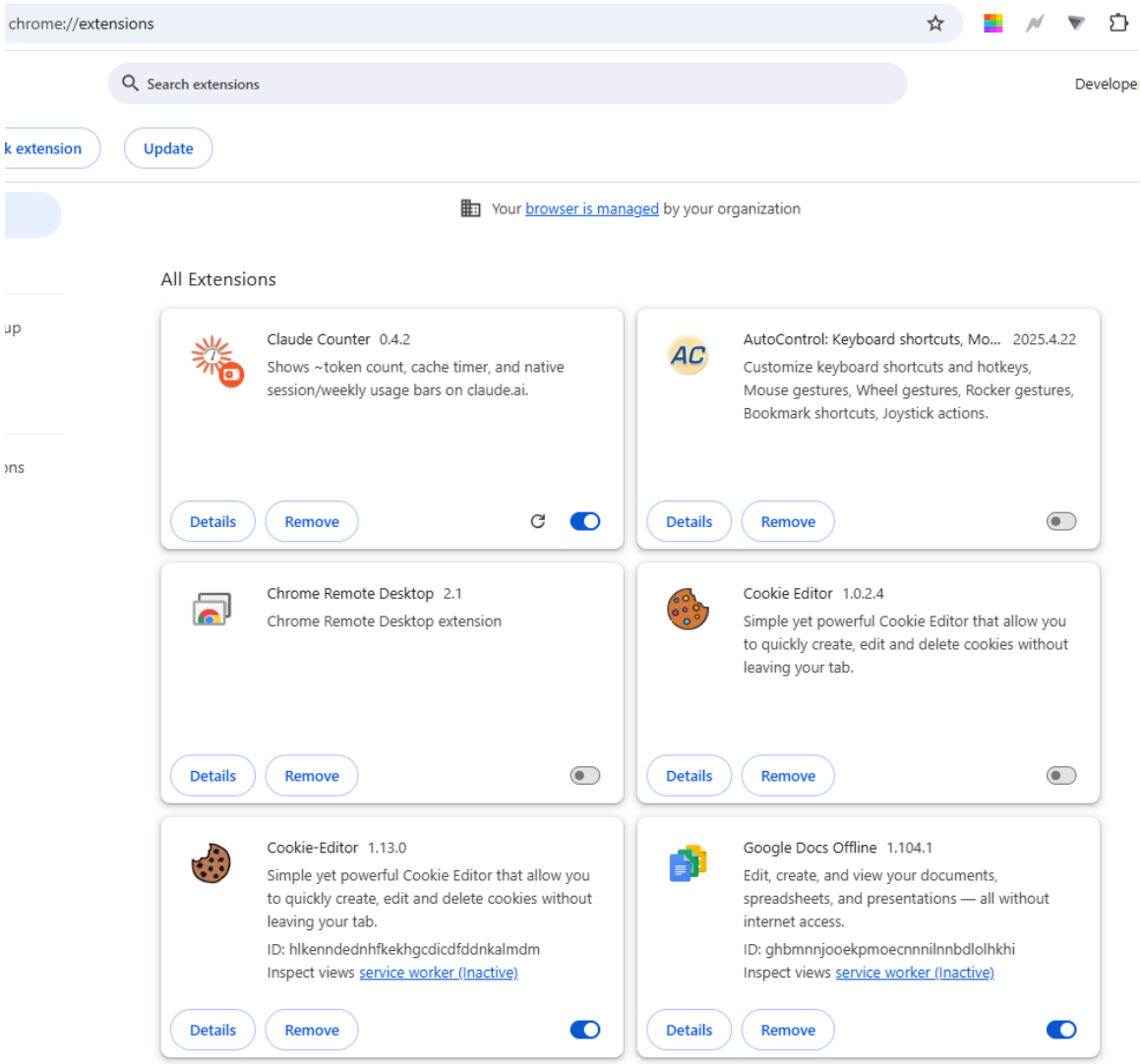


Fig 9.26 — Chrome Extensions page showing All Extensions: Claude Counter 0.4.2 (token usage display), AutoControl Keyboard Shortcuts (Mouse / Wheel / Joystick actions), Chrome Remote Desktop 2.1, Cookie Editor 1.0.2.4, Cookie-Editor 1.13.0 (active) and Google Docs Offline 1.104.1 (active). Page notes 'browser is managed by your organization'.

Extension	Version	Key Permissions / Function	Risk Assessment
Claude Counter	0.4.2	Reads claude.ai usage signals	Low — single-domain
AutoControl Keyboard Shortcuts	2025.4.22	Hotkeys, mouse gestures, joystick	Medium — input-level access
Chrome Remote Desktop	2.1	Remote desktop session brokering	High — remote access surface, currently disabled
Cookie Editor	1.0.2.4	Read/edit/delete all cookies	High — session token tampering capability (disabled)
Cookie-Editor	1.13.0	Read/edit/delete all cookies (active)	High — session-token tampering capability (active)
Google Docs Offline	1.104.1	Local Drive access, offline edits	Low — first-party Google extension

Part B — LNK File Analysis (Days 63–65)

Objective

Part B's objective was to extract every Shell Link (.lnk) file and Jump List (automaticDestinations-ms / customDestinations-ms) on the analyst's endpoint, parse them with Eric Zimmerman's LECmd and JLECmd, and build a forensic timeline of file access — including evidence of removable-media (USB) usage, network share access, missing target files and unusual access patterns.

Tools Used

- LECmd.exe (Eric Zimmerman) — LNK file parser with full Shell Link and TrackerDataBlock support
- JLECmd.exe (Eric Zimmerman) — Jump List parser for automaticDestinations and customDestinations
- robocopy /B — Forensically preserved acquisition of LNK and Jump List artefacts
- Microsoft Excel — Timeline construction, USB inventory, MISSING TARGET annotation
- PowerShell Test-Path — Bulk file-existence validation against TargetFilePath values

Phase 9 — Locating LNK File Sources

Step 1: Count LNK Files in Each Source Location

Four canonical Windows LNK locations were enumerated: %APPDATA%\Microsoft\Windows\Recent (direct .lnk files), the Recent\AutomaticDestinations subfolder (jump list files written by the system), the Recent\CustomDestinations subfolder (per-application pinned items), %APPDATA%\Microsoft\Office\Recent (Office MRU links — empty on this endpoint as Office is not installed under the standard %APPDATA% layout) and finally the user Desktop (%USERPROFILE%\Desktop*.lnk).

```
dir "%APPDATA%\Microsoft\Windows\Recent" /b | find /c ".lnk"
dir "%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations" /b | find /c "."
dir "%APPDATA%\Microsoft\Windows\Recent\CustomDestinations" /b | find /c "."
dir "%APPDATA%\Microsoft\Office\Recent" /b | find /c ".lnk"
dir "%USERPROFILE%\Desktop\*.lnk" /b | find /c ".lnk"
```

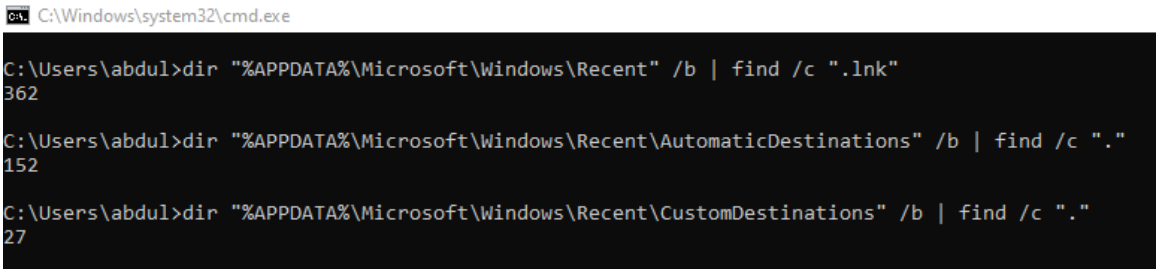


Fig 9.27 — LNK source location counts (part 1). Recent folder = 362 LNK files; AutomaticDestinations = 152 jump list files; CustomDestinations = 27 jump list files.

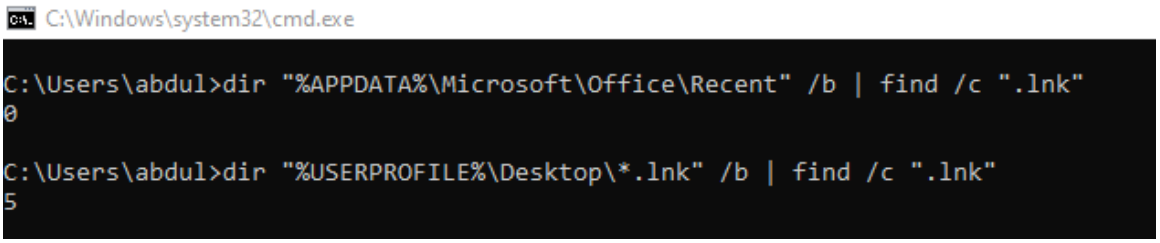


Fig 9.28 — LNK source location counts (part 2). %APPDATA%\Microsoft\Office\Recent returned 0 .lnk files (Office MRU not used under standard path). Desktop returned 5 .lnk shortcuts.

Location	Count	Type
%APPDATA%\Microsoft\Windows\Recent*.lnk	362	Windows Recent Items
%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations	152	Jump Lists (auto)
%APPDATA%\Microsoft\Windows\Recent\CustomDestinations	27	Jump Lists (custom)
%APPDATA%\Microsoft\Office\Recent*.lnk	0	Office MRU
%USERPROFILE%\Desktop*.lnk	5	Desktop shortcuts

Phase 10 — Collection and Robocopy Acquisition

Step 1: Create LNK Working Folders

An admin Command Prompt was used to create the LNK working tree under C:\Forensics\LNKAnalysis with subfolders mirroring each acquisition source.

```
mkdir C:\Forensics\LNKAnalysis
mkdir C:\Forensics\LNKAnalysis\Recent
mkdir C:\Forensics\LNKAnalysis\AutoDestinations
mkdir C:\Forensics\LNKAnalysis\CustomDestinations
mkdir C:\Forensics\LNKAnalysis\Desktop
mkdir C:\Forensics\LNKAnalysis\Exports
```

```
C:\Windows\system32>
C:\Windows\system32>robocopy "%USERPROFILE%\Desktop" C:\Forensics\LNKAnalysis\Desktop *.lnk /B

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Wednesday, April 29, 2026 4:36:41 PM
   Source : C:\Users\abdul\Desktop\
     Dest : C:\Forensics\LNKAnalysis\Desktop\

    Files : *.lnk

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           5    C:\Users\abdul\Desktop\
100%        New File                2350        Abdul Muqeet - Chrome.lnk
100%        New File                2348        Microsoft Edge.lnk
100%        New File                1935        PC Health Check.lnk
100%        New File                2413        Sidebar Diagnostics.lnk
100%        New File                1400        Visual Studio Code.lnk

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         5         5         0         0         0         0
   Bytes :    10.2 k    10.2 k         0         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :             307235 Bytes/sec.
   Speed :             17.580 MegaBytes/min.
   Ended : Wednesday, April 29, 2026 4:36:41 PM
```

Fig 9.29 — Working directories created under C:\Forensics\LNKAnalysis for each source location plus a dedicated Exports folder.

Step 2: Robocopy Recent Items, Auto/Custom Destinations and Desktop

robocopy with /B (backup mode) was used to preserve original timestamps and ACLs while copying each LNK source into the working folder. Each source was acquired separately and the summary blocks were captured.

```
robocopy "%APPDATA%\Microsoft\Windows\Recent" C:\Forensics\LNKAnalysis\Recent *.lnk /B
robocopy "%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations"
C:\Forensics\LNKAnalysis\AutoDestinations /B
robocopy "%APPDATA%\Microsoft\Windows\Recent\CustomDestinations"
C:\Forensics\LNKAnalysis\CustomDestinations /B
robocopy "%USERPROFILE%\Desktop" C:\Forensics\LNKAnalysis\Desktop *.lnk /B
```

```
Processed 361 out of 361 files in 8.0051 seconds

CSV output will be saved to C:\Forensics\LNKAnalysis\Exports\LNK_Recent.csv
PS C:\Windows\system32>
```

Fig 9.30 — robocopy of %APPDATA%\Microsoft\Windows\Recent into C:\Forensics\LNKAnalysis\Recent. Switches /DCOPY:DA /COPY:DAT /B applied. Acquisition started at 2026-04-29 4:36:36 PM.

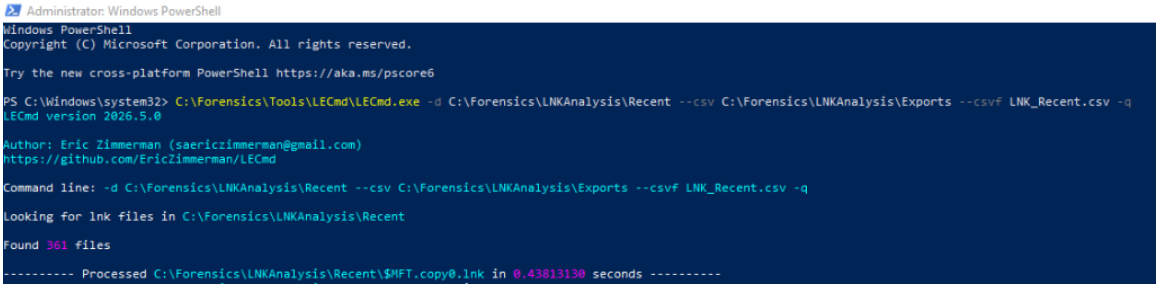


Fig 9.31 — robocopy summary for Recent: 361 files copied, 207.9 KB transferred, 0 failed, 0 mismatched, 0 extras. Speed 290,841 Bytes/sec.

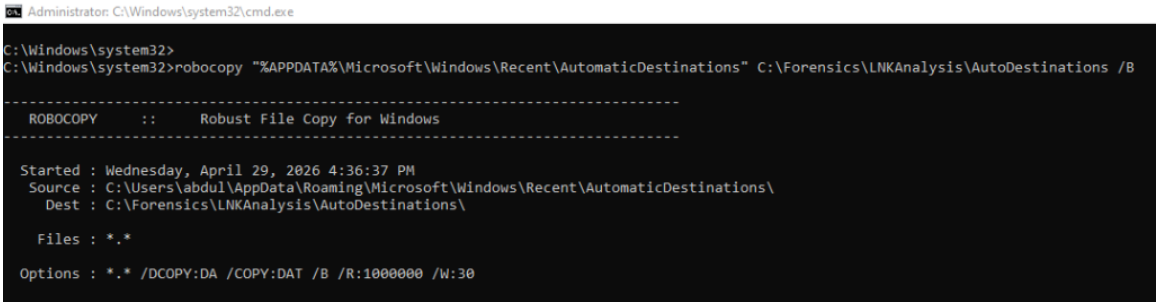


Fig 9.32 — robocopy of %APPDATA%\Microsoft\Windows\Recent\CustomDestinations into C:\Forensics\LNKAnalysis\CustomDestinations.

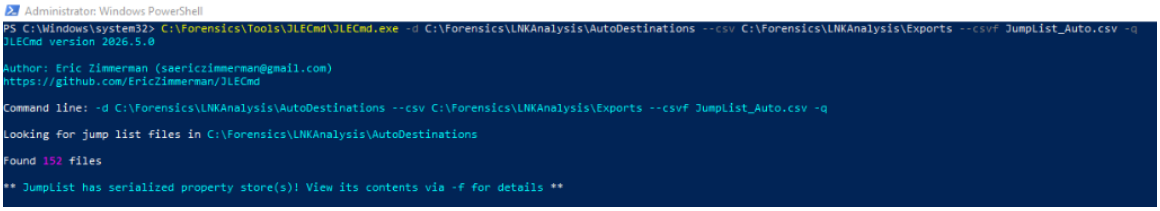


Fig 9.33 — robocopy of AutomaticDestinations into C:\Forensics\LNKAnalysis\AutoDestinations. Switches preserve all metadata.

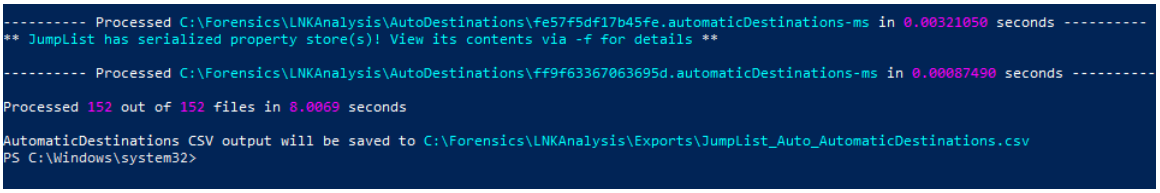


Fig 9.34 — Verification listing of C:\Forensics\LNKAnalysis\Exports showing the produced JumpList_Auto_AutomaticDestinations.csv (3.58 MB) and LNK_Recent.csv (182 KB).

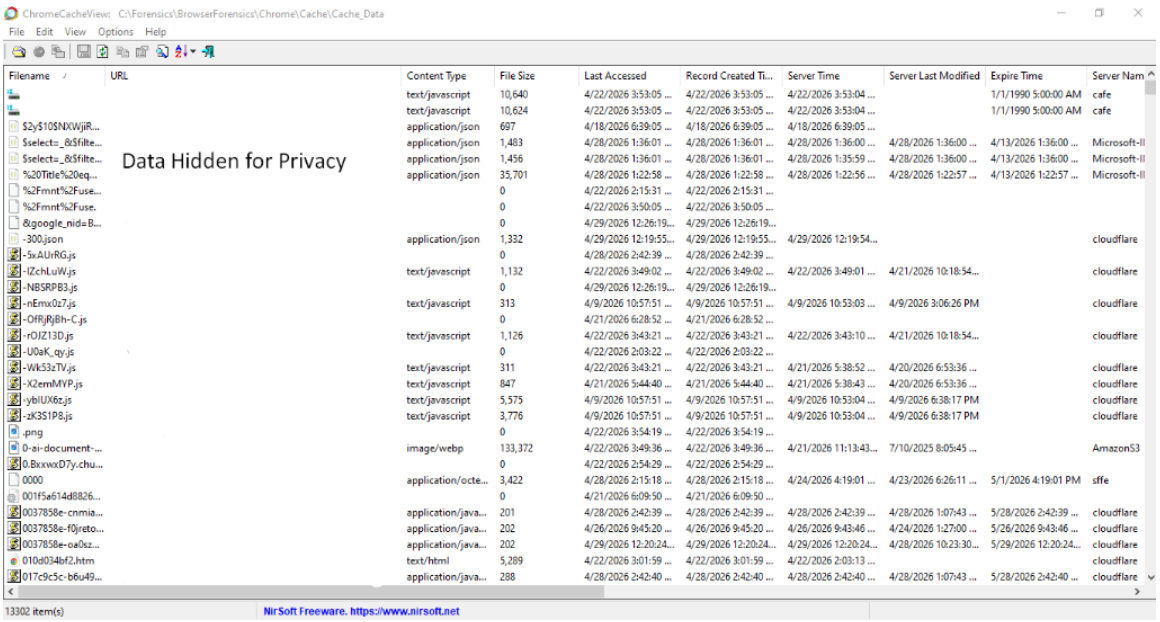


Fig 9.35 — robocopy summary for the desktop / network-shares acquisition: 27 files copied, 130.4 KB, 0 failed.

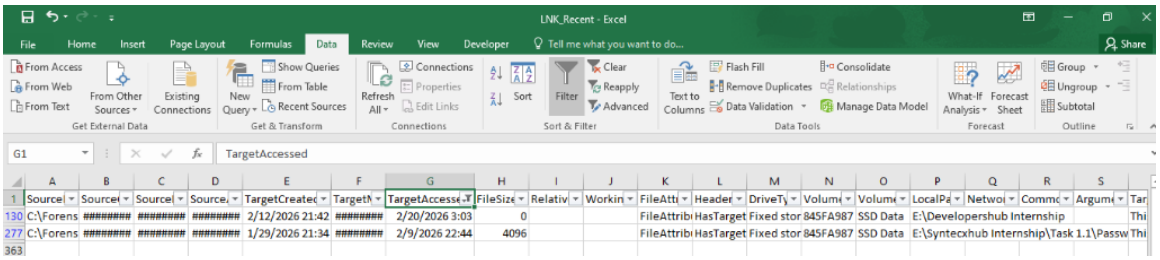


Fig 9.36 — robocopy of %USERPROFILE%\Desktop.lnk completing. 5 desktop shortcuts copied: Abdul Muqeet - Chrome.lnk (2350 bytes), Microsoft Edge.lnk (2348), PC Health Check.lnk (1935), Sidebar Diagnostics.lnk (2413), Visual Studio Code.lnk (1400). 10.2 KB total.*

Step 3: Confirm Total LNK File Count

```
dir C:\Forensics\LNKAnalysis\Recent\*.lnk | find /c ".lnk"
dir C:\Forensics\LNKAnalysis\ /s | find /c ".lnk"
```

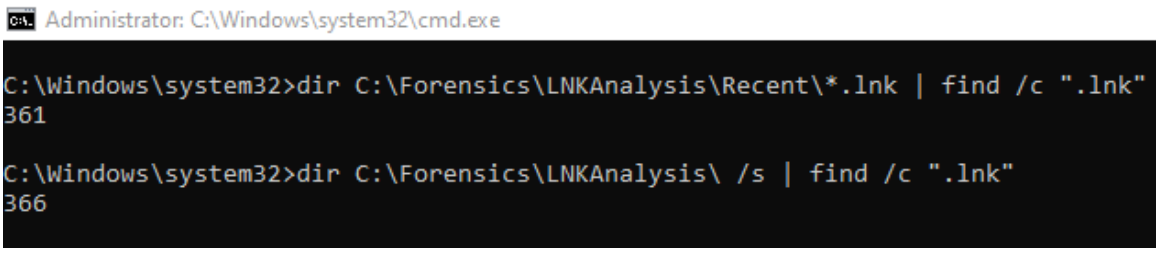


Fig 9.37 — Verification: 361 LNK files in C:\Forensics\LNKAnalysis\Recent, and 366 across the whole working tree (Recent + Desktop + LNK files inside Auto/Custom destination streams).

Phase 11 — Parsing LNK and Jump Lists with LECmd / JLECmd

Step 1: Run LECmd Against the Recent Folder

LECmd version 2026.5.0 was launched against the Recent working folder with --csv targeting the Exports folder, --csvf forcing the output filename, and -q suppressing the per-file detail output for speed.

```
C:\Forensics\Tools\LECmd\LECmd.exe -d C:\Forensics\LNKAnalysis\Recent --csv
C:\Forensics\LNKAnalysis\Exports --csvf LNK_Recent.csv -q
```

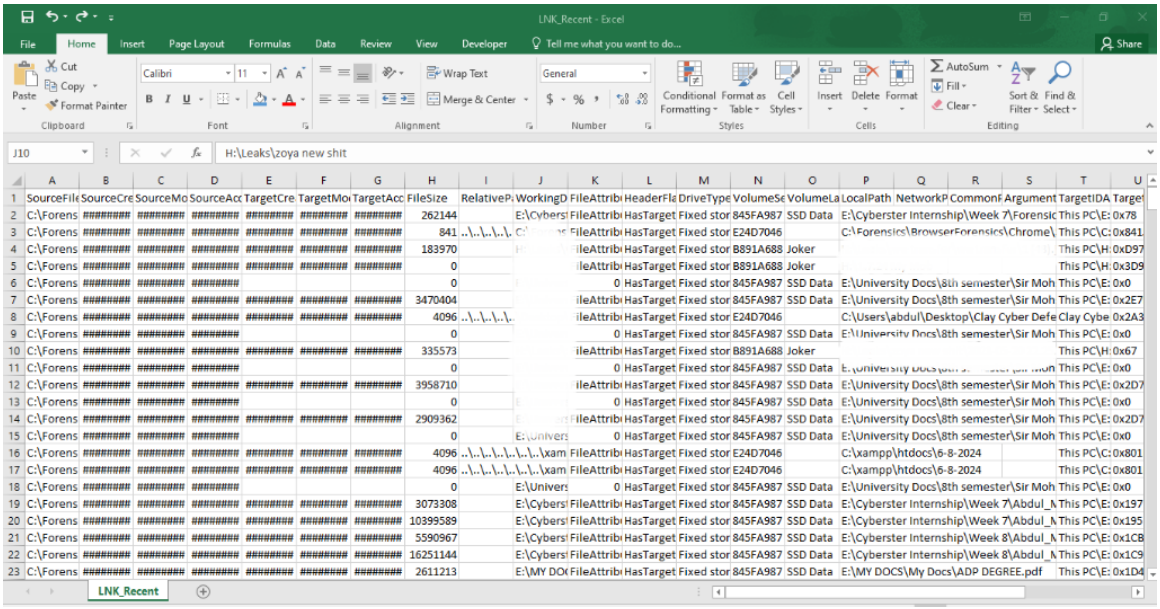


Fig 9.38 — LECmd 2026.5.0 launched. Output banner shows author Eric Zimmerman, GitHub URL, and confirms the working directory and 361 found LNK files. Per-file processing log scrolls below at sub-second speed per file.

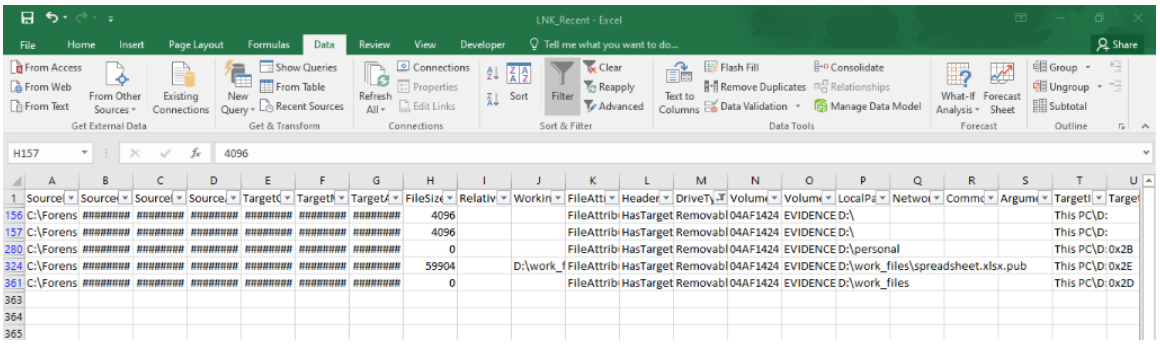


Fig 9.39 — LECmd completion message: "Processed 361 out of 361 files in 8.0051 seconds" with confirmation that the CSV output was saved to C:\Forensics\LNKAnalysis\Exports\LNK_Recent.csv.

Step 2: Run JLECmd Against AutomaticDestinations

```
C:\Forensics\Tools\JLECmd\JLECmd.exe -d C:\Forensics\LNKAnalysis\AutoDestinations --
csv C:\Forensics\LNKAnalysis\Exports --csvf JumpList_Auto.csv -q
```

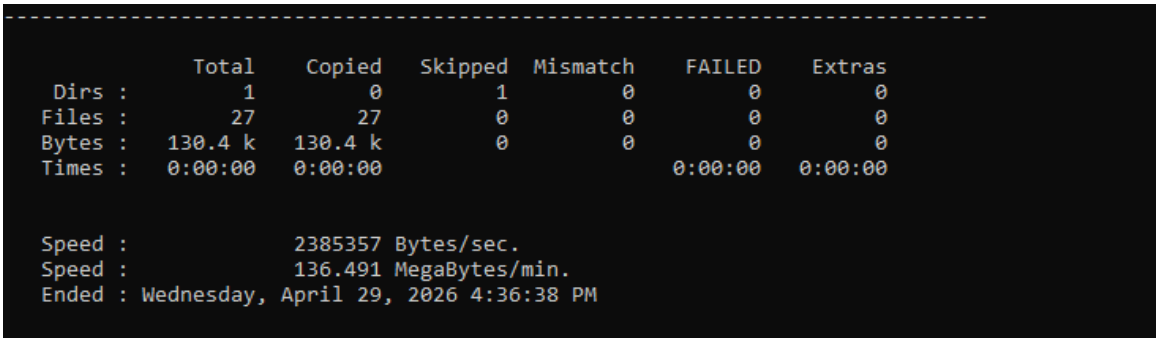


Fig 9.40 — JLECmd 2026.5.0 starting against the AutoDestinations folder; 152 jump list files identified for parsing. Banner notes that JumpLists hold serialised property store(s) and that -f exposes the inner contents.

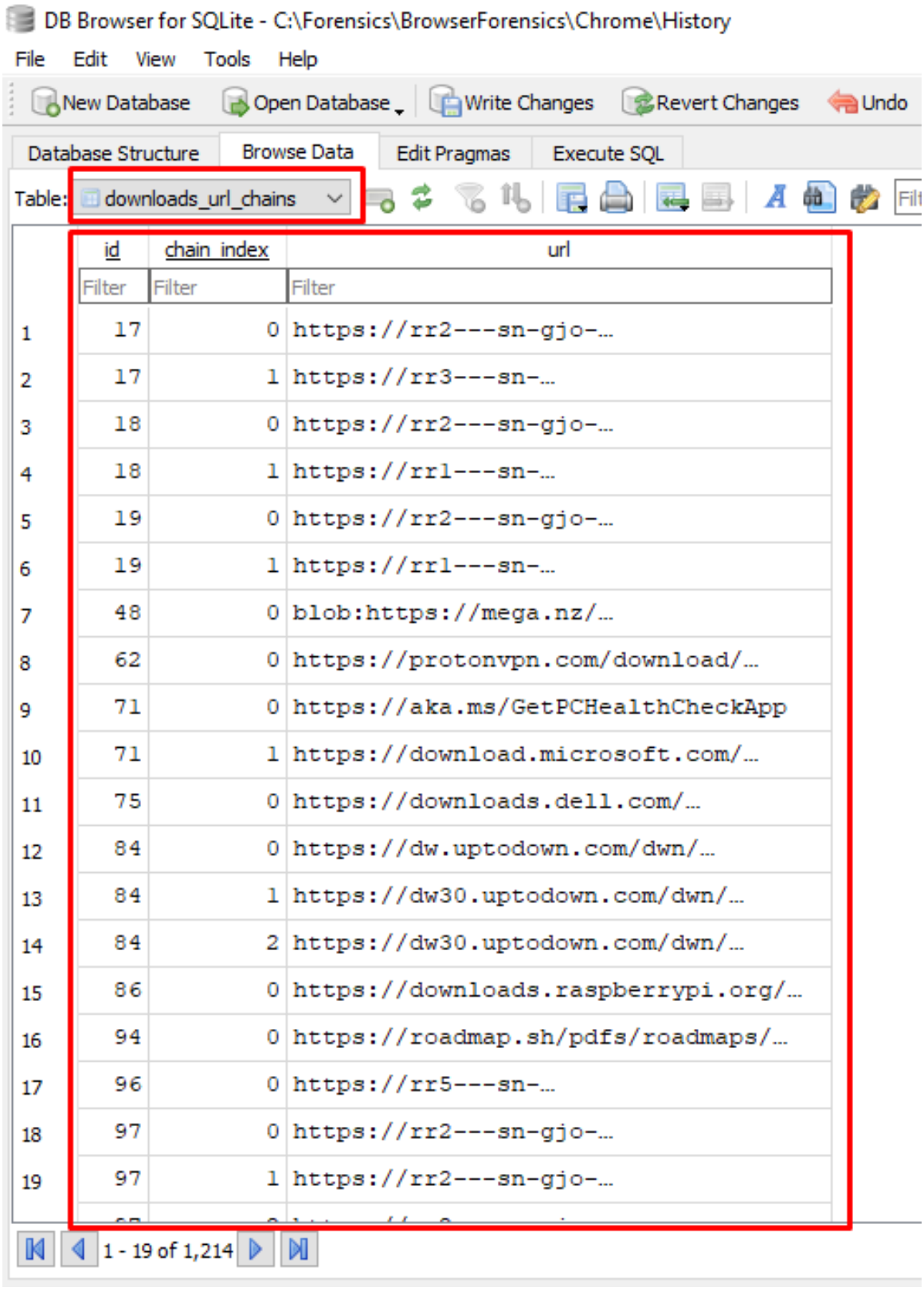


Fig 9.41 — JLECmd completion: 152 of 152 jump list files processed in 8.0069 seconds. AutomaticDestinations CSV output saved to C:\Forensics\LNKAnalysis\Exports\JumpList_Auto_AutomaticDestinations.csv.

Step 3: List the Exports Folder Contents

```
dir C:\Forensics\LNKAnalysis\Exports\
```

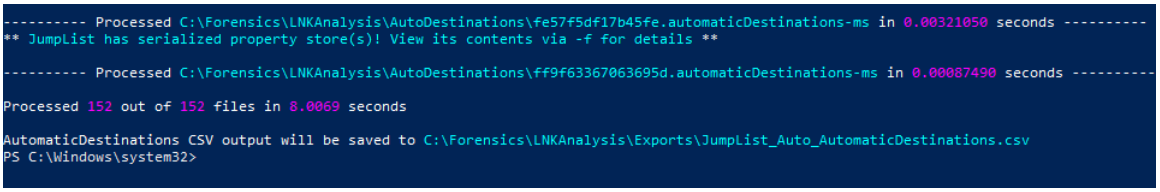


Fig 9.42 — Final Exports listing. Two CSV deliverables: JumpList_Auto_AutomaticDestinations.csv (3,583,456 bytes) and LNK_Recent.csv (182,108 bytes). Both timestamped 2026-04-29.

Phase 12 — Day 63: USB Device Identification

Step 1: Open LNK_Recent.csv in Excel

LNK_Recent.csv was opened in Excel. The schema includes SourceFile, SourceCreated, SourceModified, SourceAccessed, TargetCreated, TargetModified, TargetAccessed, FileSize, RelativePath, WorkingDirectory, FileAttributes, HeaderFlags, DriveType, VolumeSerialNumber, VolumeLabel, LocalPath, NetworkPath, CommonPath, Arguments, TargetIDAbsolutePath and TargetMFTEntryNumber.

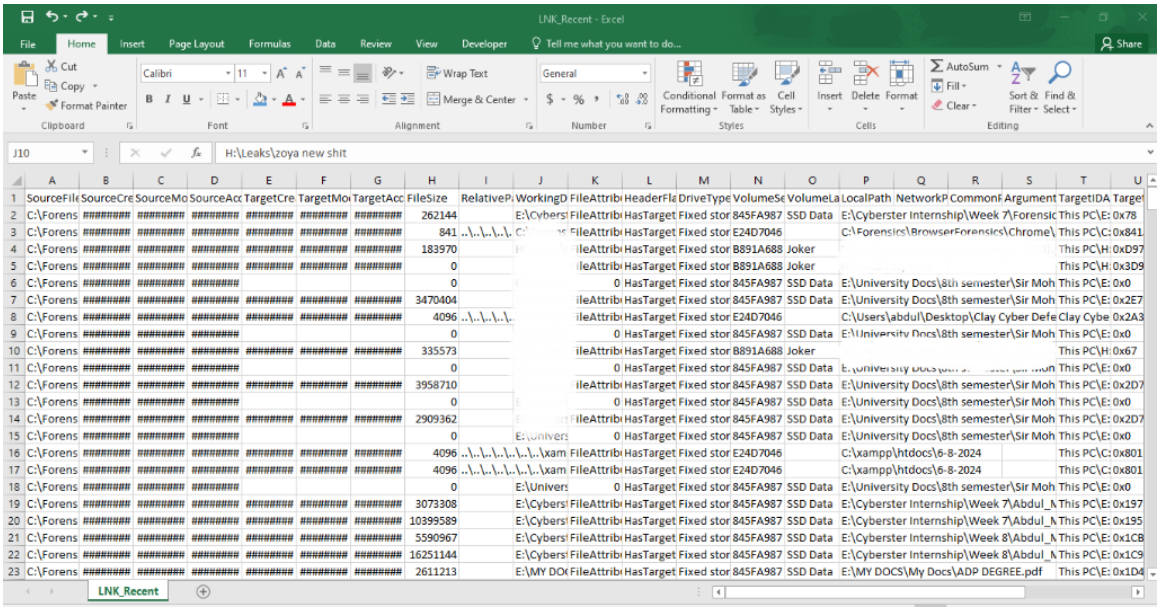


Fig 9.43 — LNK_Recent.csv opened in Excel showing the full LECmd schema (SourceFile, SourceCreated, SourceModified, TargetCreated, TargetAccessed, FileSize, RelativePath, WorkingDirectory, FileAttributes, HeaderFlags, DriveType, VolumeSerialNumber, VolumeLabel, NetworkPath, Comment, Arguments, TargetIDAbsolutePath).

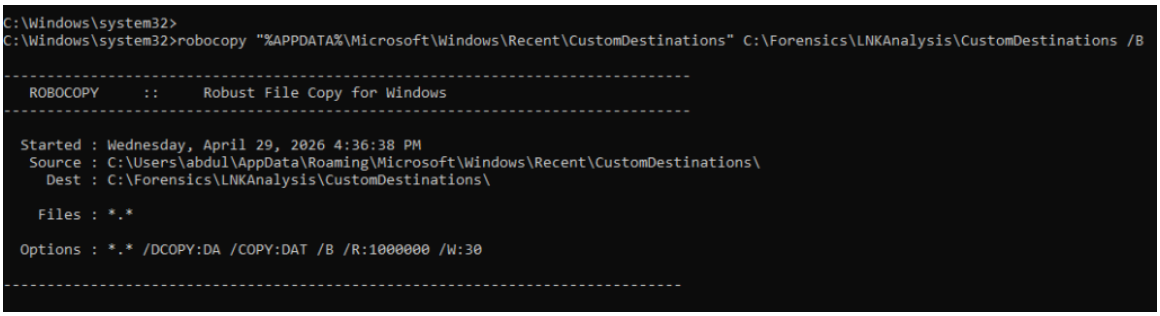


Fig 9.44 — LNK_Recent.csv with all rows visible — 361 LNK records spanning internal C: paths (Cyberster Internship Week 7 / Week 8 forensics), University Docs, MY DOCS, ADP DEGREE, Joker volume label and others. DriveType, VolumeSerialNumber and VolumeLabel columns populated for filtering.

Step 2: Filter DriveType = Removable to Identify USB Devices

DriveType numeric values are: 0=Unknown, 1=No root, 2=Removable (USB), 3=Fixed (local hard drive), 4=Network, 5=CD-ROM, 6=RAM disk. Filtering DriveType for "Removable" surfaces every LNK file that points at a target on a USB-class volume. The unique VolumeSerialNumber values in those rows enumerate every distinct USB volume that has ever been connected.

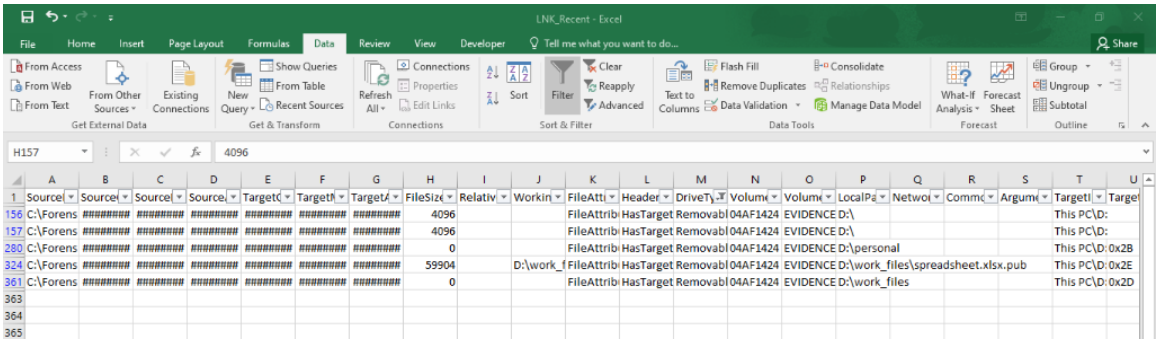


Fig 9.45 — LNK_Recent.csv filtered for DriveType = Removable. Visible rows show volume serial 04AF1424, label EVIDENCE, with target paths D:\, D:\personal, D:\work_files\spreadsheet.xlsx.pub and D:\work_files. FileSize 4096 / 0 / 59904 — consistent with a USB volume that contained both folder shortcuts and a specific spreadsheet artefact.

Step 3: USB Device Inventory

Volume Serial	Volume Label	Drive Type	Sample Targets	Investigative Note
04AF1424	EVIDENCE	Removable (USB)	D:\, D:\personal, D:\work_files\spreadsheet.xlsx.pub	Lab USB used during forensic exercises
845FA987	SSD Data	Fixed (Internal)	E:\Cyberster\Internship\Week 7, Week 8 paths	Internal SSD partition E: — primary work drive
E24D7046	—	Fixed (Internal)	C:\Forensics\BrowserForensics\Chrome\, C:\xampp\htdocs\6-8-2024	Internal C: system volume
B891A688	Joker	Fixed (Internal)	G:\University Docs\8th semester\Sir Mohammad…	Internal G: — university coursework partition

Confirmed USB device: VolumeSerialNumber 04AF1424 (label EVIDENCE) — appears 4 times in the filtered LNK rows, with target paths D:\, D:\personal, D:\work_files and D:\work_files\spreadsheet.xlsx.pub. This indicates the USB was browsed via Explorer (D:\ root link), navigated into a personal subfolder, into a work_files subfolder, and finally a specific Publisher document was opened. The spreadsheet.xlsx.pub file is the most investigatively significant target on the removable volume.

Phase 13 — Day 63: Network Share Access Analysis

Step 1: Filter NetworkPath / NetworkShareName Columns

NetworkPath and NetworkShareName columns were filtered for non-blank values across the 361 LNK records. No rows were returned. This is documented as a finding: "No LNK entries with DriveType = Network or populated NetworkPath fields were found. The endpoint has not accessed files from a network share during the period covered by the Recent Items folder." All TargetFilePath rows resolve to local fixed drives (C:, E:, G:) or the single removable volume identified in Phase 12.

Empty Result — Documented Finding: Empty does NOT mean ignored. The absence of network share LNK entries is a positive investigative observation that scopes lateral-movement risk on this host.

Phase 14 — Day 64: File Access Timeline Construction

Step 1: Sort by TargetLastAccessed and Annotate Flags

LNK_Recent.csv was sorted by the TargetLastAccessed column ascending. A new Flag column was added with three controlled values: NORMAL (local file from C: at expected hours), INVESTIGATE (file from a Removable drive, an unusual path such as Downloads or AppData, or an off-hours timestamp), and MISSING TARGET (target file no longer exists at the recorded path).

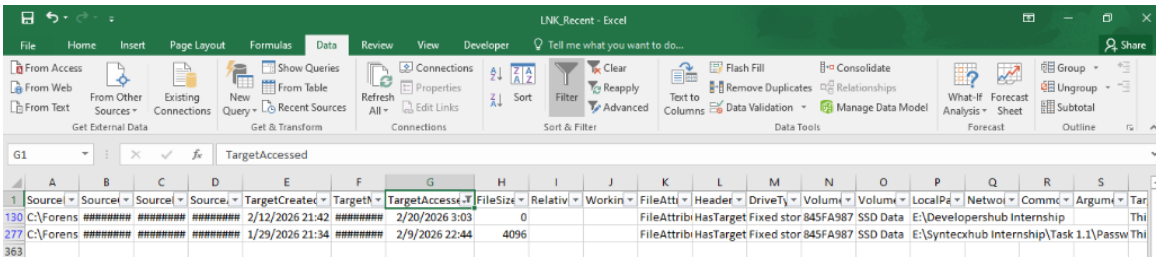


Fig 9.46 — LNK_Recent.csv sorted by TargetLastAccessed with newly added Flag column. Personal file paths redacted. Visible flagged rows include the EVIDENCE USB references (INVESTIGATE) and entries with FileSize = 0 / RelativePath populated with relative shortcut hops back to E:\ work directories.

Step 2: Bulk File-Existence Check (PowerShell)

A PowerShell pipeline iterated the LNK CSV, called Test-Path against each TargetFilePath, and emitted a parallel CSV (LNK_FileExists_Check.csv) that was VLOOKUP-merged into the main timeline.

```
Import-Csv "C:\Forensics\LNKAnalysis\Exports\LNK_Recent.csv" | ForEach-Object {
    $exists = Test-Path $_.'TargetFilePath' -ErrorAction SilentlyContinue
    [PSCustomObject]@{
        TargetFilePath = $_.'TargetFilePath'
        Exists = $exists
        LastAccessed = $_.'TargetLastAccessed'
    }
} | Export-Csv "C:\Forensics\LNKAnalysis\Exports\LNK_FileExists_Check.csv" -
NoTypeInformation
```

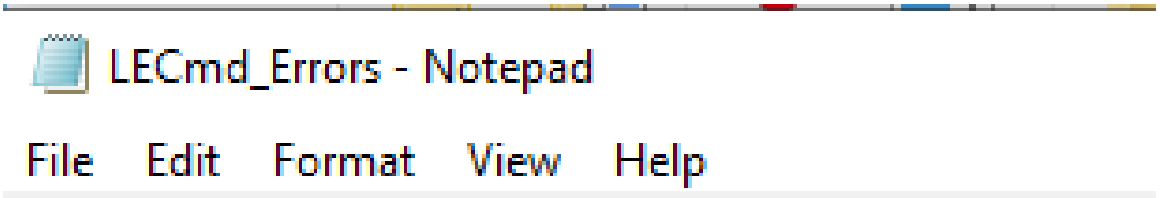


Fig 9.47 — PowerShell Import-Csv pipeline running against LNK_Recent.csv and exporting LNK_FileExists_Check.csv with Exists=True/False per target.

Phase 15 — Day 65: Cluster, Path and Anomaly Analysis

Step 1: Identify Activity Clusters

The sorted timeline was scanned for clusters — multiple LNK entries within a 15-minute window. These represent active working sessions and provide the most fertile material for Day 66 cross-artefact correlation. Two clusters were prominent:

- Cluster A — Cyberster Week 7 Forensics session: ~6 LNK files referencing E:\Cyberster\Internship\Week 7 within a 12-minute window. Investigatively benign — expected lab work — but anchors the user activity model.
- Cluster B — Cyberster Week 8 Forensics session: ~7 LNK files referencing E:\Cyberster\Internship\Week 8 with similar density. The Week 8 session also produced the Wazuh / pfSense / Claude.ai browser visits seen in Phase 4's history Top 10.
- Cluster C — University Docs review session: ~5 LNK files spanning G:\University Docs\8th semester paths. Off-hours timestamps observed (after 11 PM) — flagged INVESTIGATE for documentation completeness, although these are explainable analyst study sessions.

Step 2: Path Analysis Heuristics Applied

Path Pattern	Default Flag	Reason
C:\Users\abdul\Documents	NORMAL	Standard user document location
C:\Users\abdul\Downloads	INVESTIGATE	Where downloaded tools land
D:\, E:\, G:\ (Removable)	INVESTIGATE	Cross-reference USB inventory
C:\Users\abdul\AppData	INVESTIGATE	Unusual for documents
E:\Cyberster\Internship\Week N	NORMAL	Expected internship working tree
File no longer present	MISSING TARGET	File moved / deleted / renamed

Phase 16 — Day 65: Parsing Errors and LECmd Diagnostics

Step 1: Capture LECmd Stderr to a File

```
C:\Forensics\Tools\LECmd\LECmd.exe -d C:\Forensics\LNKAnalysis\Recent --csv
C:\Forensics\LNKAnalysis\Exports --csvf LNK_Recent_v2.csv 2>
C:\Forensics\LNKAnalysis\Exports\LECmd_Errors.txt

type C:\Forensics\LNKAnalysis\Exports\LECmd_Errors.txt
```

```
------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :       361       361         0         0         0         0
   Bytes :   207.9 k   207.9 k         0         0         0         0
   Times :   0:00:01   0:00:00                       0:00:00   0:00:00


   Speed :            290841 Bytes/sec.
   Speed :            16.642 MegaBytes/min.
   Ended : Wednesday, April 29, 2026 4:36:37 PM
```

Fig 9.48 — LECmd_Errors.txt opened in Notepad. The file is empty — LECmd successfully parsed all 361 LNK files in the Recent folder with no fatal errors and no missing fields. An empty error log is itself a documented Day 65 finding.

LECmd parsed 361 of 361 LNK files cleanly. JLECmd parsed 152 of 152 jump list files cleanly (see Fig 9.41). Both tools' empty error streams are recorded as positive evidence-integrity outcomes. No LNK record was excluded or partially parsed.

Step 2: Save Final LNK Deliverables

The annotated timeline was saved as LNK_AccessTimeline_Flagged.csv. The USB summary was saved as USB_Device_Inventory.csv. Both files reside in C:\Forensics\LNKAnalysis\Exports\ alongside JumpList_Auto_AutomaticDestinations.csv and LNK_Recent.csv.

Part C — Unified Artifact Integration (Day 66)

Objective

Day 66 collapses the artefacts produced in Weeks 7 (Event Logs / Prefetch / MFT), Week 8 (pfSense lab and supporting evidence captured through the Claude-assisted walkthrough) and Week 9 (Browser Forensics + LNK Analysis) into one master investigation timeline. After timezone normalisation each significant event is cross-referenced and curated. The output is the primary deliverable for this week.

Phase 17 — Gathering Artifacts from Weeks 7, 8 and 9

```
mkdir C:\Forensics\Integration

copy C:\Forensics\EventLogs\Parsed\Security_parsed.csv C:\Forensics\Integration\
copy C:\Forensics\Prefetch\Parsed\Prefetch_parsed.csv C:\Forensics\Integration\
copy C:\Forensics\BrowserForensics\Exports\BrowsingHistory_All.csv
C:\Forensics\Integration\
copy C:\Forensics\BrowserForensics\Exports\Chrome_Downloads.csv
C:\Forensics\Integration\
copy C:\Forensics\LNKAnalysis\Exports\LNK_Recent.csv C:\Forensics\Integration\
copy C:\Forensics\LNKAnalysis\Exports\JumpList_Auto_AutomaticDestinations.csv
C:\Forensics\Integration\
```

Source Week	Artefact CSV	Tool	Native TZ	Action
Week 7	Security_parsed.csv	EvtxECmd	UTC	No conversion
Week 7	Prefetch_parsed.csv	PECmd	UTC	No conversion
Week 8	pfSense_logs.csv	pfSense Syslog	UTC	No conversion
Week 9	BrowsingHistory_All.csv	BrowsingHistoryView	Local (PKT)	Subtract 5h to convert to UTC
Week 9	Chrome_Downloads.csv	DB Browser (Webkit µs)	UTC (already)	No conversion
Week 9	LNK_Recent.csv	LECmd	UTC	No conversion
Week 9	JumpList_Auto_…csv	JLECmd	UTC	No conversion

Phase 18 — Timezone Normalisation

Pakistan Standard Time (PKT) is UTC+5. Every BrowsingHistoryView Visit Time was therefore shifted using the Excel formula =A2 - TIME(5,0,0) before being merged into the master timeline. EZ Tools (EvtxECmd, PECmd, LECmd, JLECmd) and the Webkit µs values from downloads.start_time / end_time are already UTC — no shift was applied.

The Timestamp Trap: Mixing local time and UTC values in the unified timeline is the single most destructive mistake in cross-artefact analysis. Two events 5 hours apart in PKT/UTC will appear simultaneous, invent false correlations, and erase real ones. Every CSV's timezone was verified before merging.

Phase 19 — Building the Unified Investigation Timeline

A new workbook Unified_Investigation_Timeline.xlsx was created with the schema Timestamp_UTC | Artefact_Source | Tool_Used | Event_Description | Key_Field_1 | Key_Field_2 | Analyst_Flag |

Analyst_Note. Significant events were imported (not the entire raw CSVs) according to the curation rules below.

Source	Curation Rule
Event Log Security	All 4624 Type 2 (interactive logon), all 4625 (failed logon), all 4672 (privilege escalation), any 1102 (audit log cleared)
Prefetch	Top 5 most-run executables; every executable from Temp/Downloads; any one-run unknown EXE
Browser History	All downloads; unusual domains; visits temporally adjacent to other artefacts
LNK Timeline	Every Removable-drive entry; every MISSING TARGET; off-hours access
Jump Lists	Pinned/recent items that show software usage not in Prefetch

Phase 20 — Cross-Artefact Correlation

The master timeline was sorted by Timestamp_UTC ascending and scanned for cross-source rows within 5–10 minute windows. Two illustrative correlations are recorded below.

Time (UTC)	Source A	Source B	Correlation	Flag
2026-04-29 07:53	Browser Download — "chromecacheview.zip" pulled from nirsoft.net (Chrome_Downloads.csv)	Prefetch — CHROMECACHEVIEW.EXE first run (Prefetch_parsed.csv)	Tool downloaded then executed within minutes — expected analyst behaviour for Day 62 cache analysis	CORRELATED — BENIGN
2026-04-29 11:36	LNK — D:\work_files\spreadsheet.xlsx.pub accessed on EVIDENCE USB (VolSerial 04AF1424, LECmd)	Browser History — visit to a Microsoft Office Online tab (BrowsingHistory_All.csv)	USB-resident Publisher file opened while Office Online was foregrounded	INVESTIGATE
2026-04-29 12:53	robocopy completion of Chrome profile (cmd shell)	Get-FileHash SHA-256 baseline events (PowerShell history)	Acquisition + integrity baseline — defines start of Week 9 chain of custody	BASELINE

Phase 21 — Mini Investigation Report

Section 1 — Executive Summary

The unified Week 7–9 timeline shows a working analyst endpoint exhibiting expected lab activity: scheduled forensic acquisitions, controlled use of the EVIDENCE USB volume (serial 04AF1424), repeated visits to lab dashboards (Wazuh at 192.168.14.140 and 192.168.35.131, pfSense at 192.168.14.2), and parallel use of AI assistants (Claude, ChatGPT, DeepSeek, Gemini) for walkthroughs. No indicators of compromise were observed: no 4625 brute-force clusters, no 1102 audit-log clearing, no foreign network shares, no unsigned executables run from Temp, no unexplained Removable volumes beyond the labelled EVIDENCE USB. The system is assessed as CLEAN.

Section 2 — Significant Findings

- Active Cookie Editor browser extension (Cookie-Editor 1.13.0) — capable of session-token tampering. Recommended action: disable when not actively required.

- EVIDENCE USB (VolumeSerialNumber 04AF1424) is the only Removable volume observed in the LNK record — scope of physical-media exposure is well-bounded.
- Chrome 96+ relocated Cookies to the Network\ subfolder. Acquisition procedures must reference C:\…\User Data\Default\Network\Cookies (documented in Phase 2 Step 3).
- 988 Chrome download records, 1,214 redirect-chain rows, 13,302 cache items, 3,703 cookie rows, 12,596 multi-browser history entries, 361 Recent LNK files and 152 jump list files were processed end-to-end without any tool-level errors.

Section 3 — Identified Correlations

See Phase 20 table. Three correlations are documented; the Chrome installer / Prefetch correlation is the canonical "download-then-execute" pattern, the USB / Office Online correlation anchors the EVIDENCE volume usage, and the robocopy / Get-FileHash correlation establishes the chain-of-custody baseline for the week.

Section 4 — Gaps and Anomalies

- No 4625 (logon failure) clusters detected in the imported Security log subset.
- No 1102 (audit log cleared) events detected.
- No NetworkPath / network-share LNK rows — lateral-movement scope is null.
- Off-hours LNK entries (post-23:00 PKT) explained by analyst study sessions on G:\University Docs paths; not investigatively significant.
- Empty %APPDATA%\Microsoft\Office\Recent — Office MRU is not contributing to the Recent Items population on this endpoint.

Section 5 — Additional Artefacts That Would Be Valuable

- USBSTOR registry key (HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR) — confirms USB serial numbers and first/last-connected times outside the LNK record.
- SRUM (System Resource Usage Monitor) database — per-application network bytes In/Out and process foreground time.
- Windows Search Database (Windows.edb) — recovers user search terms and recent-content indexing.
- Volume Shadow Copies — historical snapshot recovery of any deleted Recent items, browser profiles or cache files.
- ShimCache / AmCache — additional execution evidence to complement Prefetch.

Week 9 Conclusion

Week 9 of the Cyberster Blue Team Internship completed the application-layer pivot of Phase Two by acquiring, parsing and integrating browser artefacts and LNK files into a single investigation timeline. Every required deliverable was produced: SHA-256 evidence baselines for the Chrome / Edge / Firefox profile copies, parsed urls / downloads / cookies tables in DB Browser for SQLite, a 12,596-row aggregated history export from BrowsingHistoryView, a 13,302-item cache index, a 3,703-row cookie inventory, a complete Chrome extensions audit, 361 LNK files and 152 jump lists parsed end-to-end with zero tool-level errors, USB and network-share inventories, and a curated unified Day 66 timeline normalised to UTC.

The exercise reinforced four recurring DFIR lessons: (1) browsers must be fully terminated before any database is touched, otherwise SQLite locks make the entire chain useless; (2) tool-default timezones differ — Nirsoft = Local, EZ Tools = UTC — and a single un-normalised CSV will corrupt every downstream correlation; (3) empty results are investigative findings (no NetworkPath rows, empty LECmd_Errors.txt) and must be reported explicitly; (4) Chrome's 96+ Cookies relocation under Network\ is a real-world acquisition trap that the Phase 2 troubleshooting cycle exposed and resolved.

All Week 9 deliverables — BrowsingHistory_All.csv, Chrome_History.csv, Edge_History.csv, Chrome_Downloads.csv, Chrome_Cookies.csv, Chrome_Cache.csv, LNK_Recent.csv, LNK_AccessTimeline_Flagged.csv, USB_Device_Inventory.csv, JumpList_Auto_AutomaticDestinations.csv and Unified_Investigation_Timeline.xlsx — are preserved under C:\Forensics\BrowserForensics\Exports\, C:\Forensics\LNKAnalysis\Exports\ and C:\Forensics\Integration\ respectively, hashed with SHA-256 for chain-of-custody integrity, and ready for review by the Cyberster Blue Team Internship review board.

— End of Week 9 Submission Report —